Österreichisches Informationssicherheitshandbuch

Version 4.4.0
06.11.2023

Inhalt

Zum Geleit

Die Tatsache, dass weite Bereiche des täglichen Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationen und der Informationstechnologie zunehmend in den Brennpunkt des Interesses. Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener Informationssicherheit unerlässlich.

Das nun neu überarbeitete und neu strukturierte „Österreichische Informationssicherheitshandbuch“ beschreibt und unterstützt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems in Unternehmen und der öffentlichen Verwaltung. Die grundlegende Überarbeitung und Aktualisierung seit der letzten Fassung aus 2007 führte das Bundeskanzleramt in Kooperation mit dem Zentrum für sichere Informationstechnologie - Austria (A-SIT) durch.

Diese Überarbeitung basiert einerseits auf aktuellen internationalen Entwicklungen im Bereich der Informationssicherheit und andererseits auf Kooperationen mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem schweizerischen Informatikstrategieorgan des Bundes (ISB). Dabei wird die bisherige Stärke des Österreichischen Sicherheitshandbuchs, eine eigenständige, umfassende und dennoch kompakte Darstellung von Risiken, denen Informationen ausgesetzt sind und Gegenmaßnahmen, welche für österreichische Institutionen relevant sind, weiter ausgebaut. Zusätzlich eignet sich das neue Informationssicherheitshandbuch aufgrund seiner neuen Struktur als konkrete Implementierungshilfe für nationale (E-Government) und internationale Normen (z. B. ISO/IEC 27001 und 27002) in der öffentlichen Verwaltung und der Privatwirtschaft.

Aufbau und Inhalt orientieren sich nun an internationalen Vorgaben und erleichtern damit die Umsetzung von Vorgaben aus der ISO/IEC 27000 Normenreihe. Dazu wurden Maßnahmenbausteine entwickelt, die sowohl von der öffentlichen Verwaltung als auch der Wirtschaft zielgruppenorientiert und einfach verwendet werden können. Der Aufbau des neuen Informationssicherheitshandbuchs ermöglicht auch die Berücksichtigung von Querschnittsmaterien nach Vorgabe durch Fachbereiche aus Verwaltung und Wirtschaft.

Die nun erstmals ausschließlich elektronische Umsetzung in Verbindung mit einer kontinuierlichen Wartung durch definierte Autorengruppen mit fachspezifischen Anforderungen ermöglicht eine Aktualität, die gerade in der Informationsverarbeitung besonders wichtig ist.

Österreich besitzt mit dem „Österreichischen Informationssicherheitshandbuch“ ein anerkanntes Standardwerk zur Informationssicherheit, das sich an internationalen Vorgaben orientiert und durch seine Kompaktheit auszeichnet. Es leistet einen wesentlichen Beitrag zur Erstellung und Implementierung von umfangreichen Sicherheitskonzepten in der öffentlichen Verwaltung und versteht sich als Hilfestellung für die Wirtschaft.

Vorwort und Management Summary

Zur Version 4 des Informationssicherheitshandbuchs

Herzlich willkommen bei der Lektüre der Version 4 des „Österreichischen Informationssicherheitshandbuchs“. Sie sehen hier das Ergebnis eines ehrgeizigen internationalen Projekts mit dem Ziel, dem bewährten Österreichischen Informationssicherheitshandbuch nicht nur neue Inhalte, sondern auch neue Einsatzgebiete mit Hilfe von interaktiven Funktionalitäten zu geben. Die markantesten Neuheiten sind:

- Die bisherige Struktur mit 2 Teilen wurde an die Struktur der Normen ISO/IEC 27001 und 27002 angepasst: Es gibt jetzt einen Teil mit 18 Abschnitten und einer Reihe von Anhängen. Damit wird der Einsatz als Implementierungshilfe für ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001 erleichtert.
- Die technische Realisierung unterstützt nun unterschiedliche Sprachen. Damit kann das Sicherheitshandbuch international genutzt werden.
- Gleichermaßen werden unterschiedliche Textversionen zum gleichen thematischen Inhalt für verschiedene Zielgruppen unterstützt und entwickelt.
- Eine moderne Web-Benutzeroberfläche erleichtert die Erarbeitung von lokal erzeugten Auswahl- und Checklisten mit eigenen Kommentaren. Damit können „eigene“ Sicherheitshandbücher und -policies erarbeitet werden.
- Die inhaltliche Wartung erfolgt nun kontinuierlich, um die Aktualität sicherzustellen.

Die nun vorliegende Version 4 ist die zweite Auflage in der neuen Struktur und bietet eine vollständige Wissensbasis, bestehend aus Bausteinen der bisherigen zweiteiligen Version und neu verfassten Inhalten. Aufgrund der fortschreitenden Entwicklung der Informationstechnologie wird es ein andauender Prozess sein, jeweils aktuelle Themen und Aspekte in das Informationssicherheitshandbuch einzubringen. Unbeschadet dessen sind wir für Feedbacks der Leser und Anwender dankbar.

Feedbacks zum Sicherheitshandbuch können Sie ganz einfach per E-Mail senden an: siha@a-sit.at

Bleibt noch, Ihnen für Ihr Interesse an der neuen Version zu danken und zu hoffen, dass Sie auch der Meinung sind, dass wir damit einen richtigen Weg einschlagen. Wir, das sind die Projektpartner:

- Bundeskanzleramt Österreich (BKA)

- Informatikstrategieorgan des Bundes (ISB), Schweiz
- Zentrum für sichere Informationstechnologie - Austria (A-SIT) - als Projektverantwortliche

Management Summary

Mehr denn je ist uns bewusst: Informationen sind Werte. Wir besitzen sie aus unterschiedlichen Gründen - weil wir für ihre Verwahrung oder Verarbeitung Verantwortung tragen, weil wir aus ihnen einen Vorteil ziehen, weil ihre Kenntnis uns vor Schaden bewahrt und noch viel mehr. Gehen sie uns verloren, werden sie gestohlen, sind sie falsch oder einfach nicht auffindbar, wenn wir sie benötigen, dann erleiden wir Schaden - die Palette reicht von geringfügig bis existenzbedrohend.

Das ist zwar nichts Neues, dennoch ist es der zentrale und immer wichtiger werdende Aspekt der Informationssicherheit. Niemand bestreitet das, aber wie viel sind wir bereit, in den Schutz unserer Informationen zu investieren und was ist im speziellen Fall die optimale Lösung? Hier wird es schon differenzierter, das zeigen entsprechende Umfragen immer wieder.

Aus der Fülle möglicher Bedrohungen und der Fülle möglicher Gegenmaßnahmen methodisch diejenigen identifizieren zu helfen, welche für ein spezielles Szenario beachtet werden sollen bzw. müssen, war von Beginn an die Zielsetzung dieses Handbuchs. Ausgehend von seiner ersten Version („IT-Sicherheitshandbuch für die öffentliche Verwaltung“), die sich am Sicherheitsbedürfnis öffentlicher Einrichtungen orientiert hat, wurde beim „Österreichischen Informationssicherheitshandbuch“ zunehmend dem steigenden Interesse aus der Wirtschaft Rechnung getragen.

Weiterentwicklungen betreffen primär die Inhalte: Ist es doch die rasante Entwicklung im Bereich der Informationstechnologie (IT), welche sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft zu bemerkenswerten Innovationsschüben führt, sowohl für die rechtmäßigen BesitzerInnen der Information wie auch für die potenziell unrechtmäßigen. Es gibt nicht nur immer wieder neue Technologien, sondern auch völlig neue Anwendungsgebiete wie z. B. E-Government. Die steigende Vernetzung führt dazu, dass Information „ortslos“ wird - es ist unerheblich wo sich die NutzerInnen gerade physisch befinden.

Zugleich steigt das Risikopotenzial weiter. Am Beispiel der Spam-E-Mails kann man erkennen, wie schnell ein zunächst harmlos erscheinendes Phänomen zu einem massiven Problem wurde. Und schließlich ist es immer noch die Person, der besonderes Augenmerk zu schenken ist - sie entwickelt sich nicht so rasant weiter wie die Technik; auf „typische“ Verhaltensmuster ist Verlass - sonst wären E-Mail-Würmer oder Phishing-Angriffe nicht so problematisch - obwohl die Mehrheit der BenutzerInnen über die Gefahren Bescheid weiß.

Ein Sicherheitshandbuch erfüllt seinen Zweck nur, wenn es regelmäßig der aktuellen Entwicklung Rechnung trägt und daher immer wieder überarbeitet, ergänzt und ggf. neu ausgerichtet wird. Mit dieser Motivation wurden mit der nun vorliegenden Version neue Wege beschritten:

- Ein wesentliches Einsatzgebiet ist die Implementierung der für Informationssicherheit wichtigen Normen ISO/IEC 27001 und 27002. Daher wurde die Kapitelstruktur weitgehende diesen Normen angepasst, und es wird in den Texten auf passende Normvorschriften hingewiesen.
- Mit einer modernen Benutzeroberfläche kann sowohl einfach durch die Themen geblättert, aber auch eigene Auswahl- und Checklisten („eigene“ Sicherheitshandbücher und -policies, Schulungsunterlagen) erzeugt werden.
- Die inhaltliche Wartung erfolgt ab jetzt nun kontinuierlich, um die Aktualität sicherzustellen.
- Es werden unterschiedliche Sprachen unterstützt.

Kernelemente des Informationssicherheitshandbuchs sind
der Aufbau, die Umsetzung und die Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS). Ein solches ist in ISO/IEC 27001 definiert als „[…] Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt“ bzw. enthält das Managementsystem die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation. (ISO/IEC 27001:2013, Begriffe unter Punkt 3)

Informationssicherheit entsteht nicht von selbst aus Technik oder Know-how, sondern zunächst aus dem Bewusstsein des Managements und der MitarbeiterInnen einer Organisation, dass Informationen schützenswerte und gefährdete Werte für alle Beteiligten darstellen. Daher sind auch kontinuierlich Anstrengungen und Kosten für Informationssicherheit in Kauf zu nehmen, um sie zu erhalten. Es ist aber auch bei der Informationssicherheit nicht sinnvoll, über das Ziel zu schießen: 100 % Sicherheit ist nicht erreichbar, wie viel man auch investiert.

Die für das Informationssicherheitsmanagementsystem (ISMS) relevante Norm ISO/IEC 27001 beschreibt Informationssicherheit als „kontinuierlichen Verbesserungsprozess“ (KVP):

- Planen (Plan): Festlegen des ISMS; also relevante Sicherheitsziele und -strategien ermitteln, eine organisationsspezifische Informationssicherheitspolitik zu erstellen und spezifisch geeignete Sicherheitsmaßnahmen auswählen.

- Durchführen (Do): Umsetzen und Betreiben des ISMS; also Sicherheitsmaßnahmen realisieren, für ihre Einhaltung sorgen und Informationssicherheit im laufenden Betrieb inklusive in Notfällen zu gewährleisten.
- Prüfen (Check): Überwachen und Überprüfen des ISMS auf seine Wirksamkeit; das bedeutet Vorhandensein, Sinnhaftigkeit, Einhaltung der Sicherheitsmaßnahmen zu überprüfen, aber auch Kenntnis über Vorfälle sowie üblicher Good-Practices zu erlangen.
- Handeln (Act): Instandhalten und Verbessern des ISMS; das bedeutet auf erkannte Fehler, Schwachstellen und veränderte Umfeldbedingungen zu reagieren und die Ursachen für Gefährdungen zu beseitigen. Dies bedingt erneutes Planen, womit sich ein ständiger Kreislauf schließt.

Inhalt und Struktur des Informationssicherheitshandbuchs sind an die ISO/IEC-Normen 27001 und 27002 angepasst:

- ISO/IEC 27001 (Informationssicherheitsmanagementsysteme – Anforderungen) beschreibt die für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheitsmanagementsystems relevanten Anforderungen. Im Informationssicherheitshandbuch wird darauf in den Kapiteln 2 und 3 Bezug genommen: sie beschreiben den grundlegenden Vorgang, Informationssicherheit in einer Behörde, Organisation bzw. einem Unternehmen zu etablieren und bieten konkrete Anleitungen den umfassenden und kontinuierlichen Sicherheitsprozess zu entwickeln.
- ISO/IEC 27002 (Leitfaden für das Informationssicherheitsmanagement) beschreibt konkrete Empfehlungen für Aktivitäten zur Realisierung der Maßnahmenziele. Im Informationssicherheitshandbuch beziehen sich die Kapitel 4 bis 18 darauf und entsprechen in ihrer Thematik auch den Kapiteln der Norm. Es werden hier konkrete und detaillierte Einzelmaßnahmen mit Anleitungen zu ihrer korrekten Implementierung auf organisatorischer, personeller, infrastruktureller und technischer Ebene beschrieben. Damit können den spezifischen Bedrohungen angemessene Standardsicherheitsmaßnahmen für Informationssysteme und Informationen entgegengesetzt werden. Es wird auch besonders auf die spezifisch österreichischen Anforderungen, Regelungen und Rahmenbedingungen, aber auch auf die durchgängige Einbeziehung des gesamten Lebenszyklus der jeweiligen Systeme, von der Entwicklung bis zur Beendigung des Betriebs, eingegangen.

Ein eigener Abschnitt im Anhang A beschreibt national relevante Sicherheitsmaßnahmen, die nicht in den ISO-Normen abgedeckt sind, wie beispielsweise die „Industrielle Sicherheit“ - dargestellt wird hier die Unterstützung für die Erstellung einer Sicherheitsunbedenklichkeitsbescheinigung und eine Übersicht aller für industrielle Sicherheit relevanten Vorgabedokumente aus dem nationalen, dem EU- und dem NATO-Bereich.

In den Anhängen finden sich schließlich ausgewählte Technologie- und Szenariobeschreibungen sowie Musterdokumente, Literaturhinweise und Hilfsmittel wie Referenzen.

Ausrichtung und Umfang

Von der Ausrichtung versteht sich das Informationssicherheitshandbuch nach wie vor als Sammlung von Leitlinien und Empfehlungen für die Praxis, die entsprechend den spezifischen Anforderungen und Bedürfnissen in einer Einsatzumgebung angepasst werden müssen. Dies wird auch durch die Online-Funktionalitäten wie Checklisten unterstützt. Es soll eine Ergänzung zu den bestehenden Regelungen und Vorschriften (Datenschutzgesetz, Informationssicherheitsgesetz, Verschlusssachenvorschriften, Amtsgeheimnis, …) darstellen und setzt diese weder außer Kraft noch steht es zu ihnen im Widerspruch.

Sein Umfang soll nach wie vor zwei an sich gegenläufige Aspekte vereinen:

- Die Themen sollen ausreichend konkret und detailliert dargestellt werden, um sie auch in der Tiefe zu verstehen und Maßnahmen (etwa Produkte auswählen, Vorgaben entwickeln) implementieren zu können.
- Es soll aber auch möglich bleiben, das Gesamtwerk oder größere Teile am Stück zu lesen.

Abschließend drei managementrelevante Passagen (aus Kapitel 3):

- „Zur Verantwortung der Managementebene gehört neben der Erreichung der geschäftlichen wie unternehmenspolitischen Ziele auch der angemessene Umgang mit Risiken. Sie müssen so früh wie möglich erkannt, eingeschätzt, bewertet und durch Setzen geeigneter und nachhaltiger Maßnahmen auf einen minimalen und akzeptierten Rest reduziert werden. Wegen der immer höheren Abhängigkeit von Information gilt dies besonders für Risiken aus fehlender oder mangelhafter Informationssicherheit.“
- „Es ist daher eine Managementverantwortung, einen systematischen und dauerhaften Sicherheitsmanagementprozess zu etablieren, zu steuern und zu kontrollieren“
- „Ein angestrebtes Sicherheitsniveau ist nur dann sinnvoll, wenn es sich wirtschaftlich vertreten lässt und mit den verfügbaren personellen, zeitlichen und finanziellen Ressourcen auch erreicht werden kann.“

Hauptquellen und Danksagungen

Schon lange wurden und werden auf nationaler und internationaler Ebene immer mehr Anstrengungen unternommen, einheitliche methodische Vorgehensweisen zur Etablierung von Informationssicherheit sowie Standardmaßnahmenkataloge zu erarbeiten. Davon sind die Normenreihe ISO/IEC 27000 und der Grundschutz des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) wohl die bekanntesten und bedeutendsten. Ebenso etabliert ist die Arbeit von MELANI (Melde- und Analysestelle Informationssicherung) in der Schweiz und CASES (Cyberworld Awareness Security Enhancement Structure; Luxembourg) in Luxemburg. Im Informationssicherheitshandbuch wurde diesen internationalen Entwicklungen so weit wie möglich Rechnung getragen und auf einige dieser bewährten Quellen zurück gegriffen, wie dann in den einzelnen Textbausteinen auch angeführt. Weiters waren auch die Vorgabedokumente der EU und NATO für Informationssicherheit maßgeblich.

Ausgesprochenen Dank sprechen wir den Organisationen und ihren maßgeblichen Partnern aus, die uns nicht nur ihre Zustimmung zur Nutzung ihrer Unterlagen gegeben, sondern uns bei der Erarbeitung immer wieder mit Rat und Ermunterung unterstützt haben:

- Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Deutschland;
- Informatikstrategieorgan des Bundes (ISB), Bern, Schweiz;
- Ministére de l'Economie et du Commerce extérieur, Luxembourg

1 Einführung

1.1 Das Informationssicherheitshandbuch

1.1.1 Ziele des Informationssicherheitshandbuchs

Das „Österreichische Informationssicherheitshandbuch“ positioniert sich in der Mitte zwischen den normativen Vorgaben der ISO/IEC-Normen 27001/27002 und verwandter Standards sowie der Fülle an sehr detaillierten Leitfäden und Handbüchern zur Informationssicherheit, beispielsweise den Grundschutzstandards und -bausteinen des BSI. Einerseits ist es durchaus im Stil einer Vorschrift formuliert, um notwendige Überlegungen und Maßnahmen klar und unzweifelhaft darzustellen, andererseits bietet es eine Auswahl an Möglichkeiten und Entscheidungskriterien für die Implementierung in der Praxis. Dabei wurde allerdings auf die gebotene Kompaktheit geachtet.

Implementierungshilfe zu ISO/IEC 27001:

Viele Organisationen müssen oder wollen IT-Sicherheit gemäß der Norm ISO/IEC 27001 und nachgelagerter Normen etablierten bzw. sicherstellen und ggf. auch zertifizieren lassen. Das Sicherheitshandbuch bietet dazu:

- Gemäß der Norm geordnete Interpretation der Vorgaben und Prozessbeschreibungen, um den Sicherheitsmanagement-Prozess zu etablieren und aufrecht zu erhalten: „welche Überlegungen sind anzustellen, welche Aktivitäten sind zu planen und zu entscheiden, wo ist Kontrolle nötig?“
- einen Katalog von konkreten Sicherheitsmaßnahmen, die ausgewählt, umgesetzt und eingehalten werden sollen: „was gibt es dazu, wie wird es gemacht, worauf ist zu achten?“

Hier ermöglicht es die Auswahl- und Checklistenfunktionalität etwa, ein „maßgeschneidertes“ Sicherheitshandbuch abzuleiten und in Kommentaren die tatsächlich notwendigen Maßnahmen zu beschreiben.

Instrument zur Schulung und Weiterbildung:

- Die Wissensbasis stellt insgesamt ein ganzheitliches und dennoch kompaktes Werk zur Informationssicherheit dar,
- hat das Potenzial zielgruppengerecht unterschiedlicher Textierungen,
- eignet sich auch zum Lesen bzw. Durcharbeiten „am Stück“,
- und eignet sich daher sowohl als Basis für Schulungs- und Weiterbildungsmaßnahmen bzw. -medien; sowohl modular als auch im Ganzen.

Dafür kann der Inhalt mit der Auswahl- und Checklistenfunktionalität auf die relevanten Themen eingeschränkt und in den Kommentaren etwa Fragen und Antworten dargestellt werden.

Hilfsmittel für Self-Checks:

Als Hilfsmittel für Audits, aber auch einfach zur Selbstkontrolle können die notwendigen Schritte und Maßnahmen ausgewählt und dann mit der Checklistenfunktion der Grad der Erfüllung mitsamt Begründungen festgehalten werden.

1.1.1.1 Ziele der Online-Version

Der Relaunch als Online-Version ist motiviert einerseits von der Entwicklung und steigenden Bedeutung der Normenreihe ISO/IEC 27001/27002, andererseits von Erfahrungen und Wünschen der BenutzerInnen der bisherigen Buch-Versionen nach flexiblerer Themenauswahl sowie der Möglichkeit zur Formulierung zielgruppengerechter Textierungen. Letzteres wurde vor allem als Wunsch der Wirtschaft geäußert, gilt sinngemäß auch beispielsweise für Schulen. Mit einer Neugestaltung der Datenstruktur und neu entwickelten Zugriffs- und Darstellungsmodulen wurde dem Rechnung getragen.

Es hat sich gezeigt, dass das „Österreichische Informationssicherheitshandbuch“ auch in anderen Ländern beachtet wird. Speziell aus der Schweiz kam der Vorschlag, die Möglichkeit für länderspezifische Varianten - wobei Basiswissen gemeinsam verwaltet werden soll - zu schaffen. Damit verknüpft ist konsequenterweise die Mehrsprachigkeit. Somit kam es auch zur Mitwirkung des schweizerischen ISB am Relaunch-Projekt.

Wichtigstes Ziel der Neuauflage ist selbstverständlich, die Verwendung und Verbreitung des Informationssicherheitshandbuchs zu fördern.

1.1.2 Anwendungsbereich (Scope)

Inhaltlich behandelt das vorliegende Handbuch den gesamten Bereich der Informationssicherheit. Wenn auch ein Schwerpunkt auf IT-gestützter Information liegt, wird Information dennoch umfassend gesehen: in elektronisch gespeicherter oder übertragener Form; sowie auch als schriftliche, gesprochene oder bildhaft dargestellte Informationen.

Betrachtet werden dabei auch die Sicherheit von Hardware und Software, die zur Speicherung, Verarbeitung und Übertragung von Informationen dient, sowie organisatorische, bauliche und personelle Fragen, soweit sie in direktem Zusammenhang mit der Sicherheit von IKT-Systemen und den von ihnen verarbeiteten Informationen stehen.

Die Abgrenzung zu verwandten Gebieten, wie Brandschutz, Objektsicherheit, Sicherheit von kritischen Infrastrukturen oder Datenschutz kann nicht immer eindeutig sein, oft gibt es Überschneidungen zwischen den einzelnen Themen. Ist es doch ein Ziel des Handbuchs, Problem- und Lösungspotenzial aus der und für die Praxis zu geben.

Empfehlungen für bestimmte Produkte werden nicht gegeben, und nach Möglichkeit werden Produkt- und Markennamen vermieden. Ausnahmen gibt es allerdings dort, wo die Durchdringung so groß ist, dass das Produkt schon ein Synonym für die Implementierung darstellt, oder ein Produkt ausgesprochen spezifische Sicherheitseigenschaften aufweist bzw. kostenlos angeboten wird.

1.1.3 Neuheiten der Version 4

Struktur

Anpassung an ISO/IEC 27001/27002: Anstelle der bisher 2 Hauptteile (Sicherheitsmanagement und Sicherheitsmaßnahmen) gibt es jetzt nach dem Management-Summary 18 Abschnitte und eine Reihe von Anhängen:

- Abschnitt 1 ist eine Einführung sowohl für die Handhabung des Handbuchs als auch in die grundsätzliche Thematik,
- Abschnitte 2 und 3 beschreiben die für Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheitsmanagementsystems relevanten Anforderungen gemäß ISO/IEC 27001 4, 5, 6, 7, 8): es handelt sich dabei um den grundlegenden Vorgang, Informationssicherheit in einer Behörde, Organisation bzw. einem Unternehmen zu etablieren und diese Abschnitte bieten konkrete Anleitungen, den umfassenden und kontinuierlichen Sicherheitsprozess zu entwickeln.
- Abschnitte 4 bis 18 beschreiben die konkreten Sicherheitsmaßnahmen inkl. der Aktivitäten zu ihrer Umsetzung und Einhaltung. Sie entsprechen in ihrer Reihenfolge und generellen Thematik den Empfehlungen gemäß ISO/IEC 27002 bzw. dem Anhang zu ISO/IEC 27001 - allerdings gibt es keine 1:1-Entsprechung auf der Ebene der einzelnen Details (Textbausteine). Sie erörtern konkrete und detaillierte Einzelmaßnahmen und Anleitungen zu ihrer korrekten Implementierung während ihres gesamten Lebenszyklus auf organisatorischer, personeller, infrastruktureller und technischer Ebene. Es wird allerdings auch auf spezifisch österreichische Anforderungen, Regelungen und Rahmenbedingungen eingegangen.
- In den einzelnen Themenbausteinen werden - sofern zutreffend - Bezüge zu den jeweils zugehörigen Kapiteln der ISO/IEC-Normen 27001 und 27002 dargestellt.
- In den Anhängen finden sich ausgewählte Szenarien und Technologien losgelöst von zu setzenden Maßnahmen, Muster für Verträge, Anweisungen, Referenzen zu Normen, Gesetzen und verwandter Literatur sowie Quellenhinweise.

Damit geht eine neue Nummerierung der Kapitel und Textbausteine einher.

Inhalte

- Um alle Themen laut ISO/IEC 27001/27002 abzudecken, gibt es nun neue Kapitel bzw. Themenbausteine etwa zu „Outsourcing“, „Umgang mit Vermögenswerten“, „Interne Audits“, „Verbesserungsprozess“
- Neue und geänderte Themenbausteine zu veränderten Technologien oder Gefährdungen werden nunmehr kontinuierlich eingearbeitet bzw. obsolete eliminiert.

Datenbasis (Online-Version)

- Jeder Textbaustein kann künftig in mehreren unterschiedlichen Ausprägungen (Formulierungen, Vereinfachungen) vorhanden sein und mittels Filteroptionen ausgewählt werden. Damit werden zielgruppenorientierte Darstellungen unterstützt.
- Filteroptionen werden sowohl für Einsatzgebiete (z. B. Government/Wirtschaft) als auch für Rollen Leserkreise (z. B. Management/Wartungspersonal/ BenutzerInnen) entwickelt. Die Filterregeln sind nicht a priori festgeschrieben, sondern Gegenstand von Vereinbarungen (in zentralen Autorengruppen oder individuellen Implementierungen) und damit flexibel für Erweiterungen.
- Mit Filteroptionen werden auch unterschiedliche Sprachen ermöglicht.
- Links zu österreichischen Gesetzen führen direkt zum entsprechenden Gesetzestext im Rechtsinformationssystem (RIS).
- Die Datenbasis besteht aus einem Satz von XML-Dateien (extended Markup Language), die mittels geeigneter Transformationen in andere gängige Darstellungs- (HTML - Hypertext Markup Language) oder Textformate (RTF - Rich Text Format, PDF - Portable Document Format) umgewandelt werden können.

Funktionalität (Online-Viewer)

Der neu entwickelte Online-Viewer läuft in einem Standard-Browser und benötigt abgesehen vom Vorhandensein einer Javascript-Unterstützung keine Installation. Er bietet als Hauptfunktionalitäten:

- Blättern (Browse) im Sicherheitshandbuch: Das kann seriell vom Anfang bis zum Ende, aber auch durch gezielten Sprung auf Kapitel oder Textbausteine erfolgen.
- Filteroptionen für Einsatzgebiete, Branchen, Rollen, Leserkreise sowie unterschiedliche Sprachen.
- Zusammenstellung einer Liste, das heißt einer individuellen Auswahl von Themen (ganze Kapitel, Unterkapitel oder Textbausteine). Sie kann lokal abgespeichert und wieder geladen werden.

- Zusammenstellung einer Checkliste, das ist eine individuelle Auswahl mit der Möglichkeit, pro Textbaustein Checkboxen anzukreuzen sowie Kommentare zu verfassen und lokal abzuspeichern. Einsatzgebiete für Auswahl- oder Checklisten sind beispielsweise das Erstellen eigener Policies, Schulungsunterlagen, Statusberichte (Erfüllungsgrad von Maßnahmen), Self-Checks und Querschnittsmaterien.
- Druck von Auswahl- oder Checklisten (Online-Version).
- Transformation von Auswahl- oder Checklisten in PDF-Textdateien.

Update Funktion

Mit ihrer Hilfe können lokal abgespeicherte und verwendete Auswahl- oder Checklisten aktuell gehalten werden:

- Die lokale Liste enthält mehrere Kapitel oder Bausteine aus der Wissensbasis, die sich inzwischen geändert haben könnten (anhand ihrer jeweiligen Versionsnummer).
- Beim Blättern in der Liste wird ein entsprechender Warnhinweis gegeben.
- Wenn gewünscht, können die neuen Versionen aus der Wissensbasis in die lokale Liste übernommen werden.

1.1.4 Quellen, Verträglichkeiten, Abgrenzungen

Normenfamilie ISO/IEC 27000

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur Informationssicherheit entstanden. Die internationale Normenfamilie ISO/IEC 27000 gibt einen allgemeinen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge ihrer verschiedenen Einzelnormen. Es finden sich hier die grundlegenden Prinzipien, Konzepte, Begriffe und Definitionen für solche Managementsysteme.

Abbildung 1.1: Vereinfachter Überblick über die ISO/IEC 27000 Normenfamilie

Die Normenfamilie ISO/IEC 27000 besteht vereinfacht aus fünf grundlegenden Bereichen:

- Terminologie und Aufbau über ISO/IEC 27000 („Überblick und Vokabular“)
- Zertifizierbarer ISO/IEC 27001 („Anforderungen“ in Verbindung mit den Anforderungen an Audit und Zertifizierung aus ISO/IEC 27006)
- Standards im Sinne für „Allgemeine Richtlinien“ (ISO/IEC 27002 bis ISO/IEC 27005, ISO/IEC 27007 und ISO/IEC 27008)
- Spezifische Standards für ausgewählte „Branchen“ (ISO/IEC 27011, ISO/IEC 27015, ISO/IEC 27019)
- Subnormen „Supporting Standards“ (z.B. ISO/IEC 27032 für “Cyber Security”, ISO/IEC 27036 für “Outsourcing”)

Für die drei Branchen Telekommunikation, Finanzen sowie Energie sind spezifische Standards verfügbar. Diese drei Standards decken für die zuvor genannten Bereiche charakteristische Eigenschaften sowie Sicherheitsanforderungen ab. Darüber hinaus ist eine Ergänzung des Scopes für eine ISO/IEC 27001-Zertifizierung einer Organisation möglich. Davon umfasst ist beispielsweise der datenschutzrelevante Standard ISO/IEC 27701. Dieser Standard liegt als Empfehlung vor. Demzufolge dient dieser als Erweiterung der ISO/IEC 27001 im Bereich der Informationssicherheit um Datenschutzkriterien. Damit wird ein allfälliger Nachweis der Erfüllung datenschutzrechtlicher Anforderungen realisiert.

Für das vorliegende Informationssicherheitshandbuch sind insbesondere folgende Standards aus der Normenfamilie ISO/IEC 27000 relevant:

- Der Standard ISO/IEC 27001 „Information technology - Security techniques - Information security management systems - Requirements“ ist der erste internationale Standard zum Informationssicherheitsmanagement, der auch eine Zertifizierung ermöglicht. ISO/IEC 27001 gibt in 5 konkreten Kapiteln (4, 5, 6, 7, 8) allgemeine Empfehlungen für Managementaktivitäten, um ein ISMS zu planen, etablieren, zu betreiben, zu überwachen und laufend zu verbessern. Ein normativer Anhang verweist auf die Umsetzung gemäß ISO/IEC 27002; ISO/IEC 27001 bietet keine Hilfe für die praktische Umsetzung.

- ISO/IEC 27002 (vormals ISO 17799) „Information technology - Security techniques – Code of practice for information security controls“ befasst sich als Rahmenwerk für das Informationssicherheitsmanagement hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Informationssicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die erforderlichen Informationssicherheitsmaßnahmen werden eher kurz auf ca. 80 Seiten skizziert angerissen. Die Empfehlungen sind für Managementebenen formuliert und enthalten nur wenige konkrete technische Hinweise. Ihre Umsetzung ist auch nur eine von vielen Möglichkeiten, die Anforderungen des ISO/IEC-Standards 27001 zu erfüllen.
- ISO/IEC 27005 „Information technology - Security techniques - Information security risk management“ enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt er bei der Umsetzung der Anforderungen aus ISO/IEC 27001. Es wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben. ISO/IEC 27005 löst den bisherigen Standard ISO 13335-2 ab.
- Weitere Standards der ISO/IEC 27000 Reihe: Langfristig wird die Normenreihe ISO/IEC 27000 voraussichtlich aus den Standards 27000 - 27023 und 27030 - 27044 bestehen. Alle Standards dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO/IEC 27001. Die weiteren Standards sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO/IEC 27001 beitragen und beschäftigen sich beispielsweise mit der praktischen Umsetzung der ISO/IEC 27001, also der Messbarkeit von Risiken oder mit Methoden zum Risikomanagement.

Das Informationssicherheitshandbuch geht in Aufbau, Struktur und Abhandlung der generellen Themen konform mit ISO/IEC 27001 und 27002, bietet allerdings in einer kompakten Form auch technische und organisatorische Hinweise und Ratschläge zur Implementierung.

BSI Grundschutz Standards und Maßnahmenbausteine

- Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet seit 1994 zunächst mit dem Grundschutzhandbuch, später mit den Grundschutz-Standards und Maßnahmenbausteinen bzw. Grundschutz-Kompendium eine umfassende und äußerst detaillierte Informationsbasis und daraus etablierte Methoden für eine Vorgehensweise zum Aufbau einer Sicherheitsorganisation sowie für die Risikobewertung, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit.
- Sie hat sich als ganzheitliches Konzept für Informationssicherheit und als Standard etabliert; und das BSI bietet ISO/IEC 27001 Zertifizierungen nach IT-Grundschutz an. Unterschiedliche Zielgruppen werden durch jeweils separate Entwicklungen unterstützt.

Das Österreichische Informationssicherheitshandbuch wird auf Basis einer gelebten Kooperation mit dem BSI immer wieder mit neuen Entwicklungen bei den Grundschutz-Standards und -Bausteinen abgeglichen. Teilweise grenzt es sich diesen gegenüber vor allem durch eine kompaktere Darstellungsweise ab, die mittleren und kleineren Organisationseinheiten entgegenkommt und das Durcharbeiten des Informationssicherheitshandbuchs „am Stück“ nach wie vor ermöglicht. Seine neuen Funktionalitäten wie unterschiedlich formulierte Textbausteine verfolgen auf eigene Weise das Ziel der Ansprache unterschiedlicher Zielgruppen.

MELANI (Melde- und Analysestelle Informationssicherung)

Im Rahmen von MELANI wird in der Schweiz ein CERT (Computer Emergency Response Team) betrieben, aber auch auf einer Webseite Informationen über Gefahren und Maßnahmen, Checklisten, Lageberichte und Schulungsmaßnahmen geboten. Der Anspruch richtet sich auf gezielte und aktuelle Darstellung vor allem von Gefahren und Fehlverhalten, wobei keine ausgesprochenen Zielgruppen definiert sind; beispielsweise wird den Problemen, denen Banken und Finanzinstitutionen ausgesetzt sind, breiter Raum gegeben.

Das Informationssicherheitshandbuch behandelt zum Teil eine ähnliche Thematik, positioniert sich dabei stark an der Implementierung und muss dem Anspruch, sämtliche relevanten Themen anzusprechen, genügen.

CASES (Cyberworld Awareness Security Enhancement Structure)

Die vom luxemburgischen Ministerium für Wirtschaft und Außenhandel betriebene Webseite „CASES“ ist in deutscher und französischer Sprache verfügbar und richtet sich zum einen an Klein- und Mittelbetriebe, zum anderen an Schüler und deren Eltern. Auf sehr einfachen und anschaulichen Webseiten wird eine umfassende Darstellung der wesentlichsten Gefahren und Sicherheitsmaßnahmen geboten, Basistechnologien anschaulich beschrieben und auch Anleitungen zur Ausarbeitung einer Sicherheitspolitik speziell für kleine Organisationen gegeben.

Das Informationssicherheitshandbuch hat sich aus dem „IT-Sicherheitshandbuch für die öffentliche Verwaltung“ entwickelt und hat somit bisher als Zielgruppen mittlere bis größere Institutionen mit Bedarf nach knapper, aber vorschrift-ähnlicher Darstellung angesprochen. Mit Hilfe seiner neuen Funktionalitäten wie unterschiedlich formulierbarer Textbausteine und einer informell bereits aufgenommenen Kooperation werden sich nunmehr auch einige Inhalte von CASES im Informationssicherheitshandbuch finden.

1.1.5 Informations- versus IT-Sicherheit

Die Definition dieser beiden Begriffe und ihrer Abgrenzung voneinander war in den vergangenen Jahren oft Gegenstand lebhafter Diskussionen. Dabei ist auch ein gewisser Bedeutungswandel bei diesen Begriffen festzustellen:

Verstand man von einigen Jahren unter „IT-Sicherheit“ im Wesentlichen den Schutz von IT-Systemen (und damit den auf ihnen verarbeiteten Informationen) und unter „Informationssicherheit“ den Schutz von Informationen unabhängig von ihrer Darstellungsform (also elektronisch, schriftlich, bildhaft oder gesprochen), so sind diese beiden Begriffe mittlerweile fast synonym zu sehen: auch in der IT-Sicherheit sind Fragen zu behandeln, wie Information an sich geschützt werden kann (etwa wie mit Papierausdrucken von vertraulichen Informationen umzugehen ist), während umgekehrt die Sicherheit von elektronisch gespeicherten und verarbeiteten Informationen ohne die technische Sicherung der zugrunde liegenden IKT- (Informations- und Kommunikationstechnologie-) Systeme nicht zu erreichen ist.

Die Grenzen sind also fließend. International und nicht zuletzt in den Normen hat sich in den letzten Jahren eher der Begriff „Informationssicherheit“ als der umfassendere etabliert - daher auch der Name „Informationssicherheitshandbuch“.

[Quelle: BSI Leitfaden Informationssicherheit]

1.2 Informationssicherheitsmanagement

Information stellt heute sowohl für die öffentliche Verwaltung als auch für Organisationen der Privatwirtschaft einen wichtigen Wert dar. Die Erfüllung der Geschäftsprozesse ist ohne die Korrektheit, Vertraulichkeit und Verfügbarkeit der Informationen oft nicht mehr möglich. Information kann dabei in unterschiedlicher Form existieren – elektronisch gespeichert oder übertragen, geschrieben, als Bild oder in gesprochener Form. Die Tatsache, dass weite Bereiche des täglichen Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationen und der Informationstechnologie zunehmend in den Brennpunkt des Interesses.

Dabei darf sich Sicherheit nicht auf einzelne Teilaspekte, wie die Verschlüsselung vertraulicher Daten oder die Installation von Firewalls beschränken, sondern muss integraler Bestandteil eines modernen IKT- (Informations- und Kommunikationstechnologie-) Konzeptes sein. Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener Informationssicherheit unerlässlich.

Das gegenständliche Handbuch beschreibt die Vorgehensweise zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems (ISMS). Dabei wird Information unabhängig von ihrer Darstellungsform betrachtet, also elektronisch gespeicherte und verarbeitete Information genauso wie Information in schriftlicher oder gesprochener Form. Die hier dargestellte Vorgehensweise wird für die österreichische Bundesverwaltung sowie für andere Bereiche der öffentlichen Verwaltung bzw. für die Privatwirtschaft zur Anwendung empfohlen.

1.2.1 Ziele des Informationssicherheitsmanagements

Informationssicherheit entsteht nicht von selbst aus Technik oder Know-how, sondern zunächst aus dem Bewußtsein des Management und der MitarbeiterInnen einer Organisation, dass Informationen schützenswerte und gefährdete Werte für alle Beteiligten darstellen. Daher sind auch kontinuierlich Anstrengungen und Kosten für Informationssicherheit in Kauf zu nehmen, um sie zu erhalten. Es muss allerdings ebeso bewusst sein, dass 100 % Sicherheit nicht erreicht werden kann, wie viel man auch investiert. Ziel muss es also sein, ein angemessenes Sicherheitsniveau zu erreichen und dauerhaft zu erhalten.

Durch Etablieren und Erhalten eines Informationssicherheitsmanagementsystems (ISMS) sollen die grundlegenden Ziele der Informationssicherheit erreicht werden:

- Integrität: Informationen dürfen nur von den vorgesehenen Personen und Prozessen verändert werden,
- Vertraulichkeit: Informationen dürfen nur für die vorgesehenen Personen und Prozesse offen gelegt werden,
- Verfügbarkeit: Informationen müssen für die vorgesehenen Personen und Prozesse bereitgestellt sein, wenn diese sie benötigen

Das klingt selbstverständlich und einfach, ist in der Praxis allerdings eine Herausfoderungen für die Organisation, da die Informationen vielfältigsten Gefahren ausgesetzt sind:

- So ist Integrität von technischen Fehlern, unbefugten Manipulationsversuchen (auch etwa Viren, Würmer), Fahrlässigkeit etc. bedroht,
- die Vertraulichkeit ist durch Spionageaktivitäten, Datenmissbrauch, aber ebenso von Fehlern und Schlamperei gefährdet,
- die Verfügbarkeit kann von kleineren und größeren Systemausfällen (z. B. durch Brände oder Katastrophen), aber auch bewußten DoS-Attacken (Denial-of-Service) - bis zum Stillstand - reduziert werden.

1.2.2 Aufgaben des Informationssicherheitsmanagements

Informationssicherheit ist immer eine Managementaufgabe. Nur wenn die Leitung einer Organisation voll hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden.

PDCA-Zyklus

Die für das Informationssicherheitsmanagement relevante Norm ISO/IEC 27001 beschreibt Informationssicherheit als „kontinuierlichen Verbesserungsprozess“ (KVP) in einem Informationssicherheitsmanagementsystem (ISMS) nach dem „Plan-Do-Check-Act“-Modell (PDCA – „Planen, Durchführen, Prüfen, Handeln“). Dieser PDCA-Zyklus (auch: „PDCA-Modell“ oder „Demin-Cycle“) ist in der folgenden Abbildung grafisch dargestellt und beschreibt einen Kreislauf der kontinuierlich durchwandert wird.

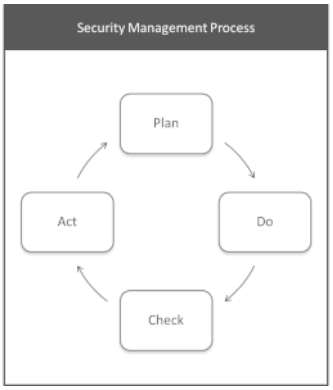

Abbildung 1.2: Die vier Phasen des PDCA-Zyklus

- Planen (Plan): Festlegen des ISMS; also relevante Sicherheitsziele und -strategien ermitteln, eine organisationsspezifische Informationssicherheitspolitik erstellen und spezifisch geeignete Sicherheitsmaßnahmen auswählen. Daraus folgt das Identifizieren, Planen, Spezifizieren und Installieren des Informationssicherheitsmanagementsystems im Rahmen der Unternehmensstrategie, den operationellen Anforderungen (z.B. Betrieb von Computersystemen) und unter Berücksichtigung rechtlicher Rahmenbedingungen. Auch Anforderungen für die Geschäftskontinuität („Business Continuity“) werden hier festgelegt. Ebenfalls erfolgt in dieser Phase die Entwicklung von Sicherheitskonzepten sowie die (z.B. zumeist risikobasierte) Auswahl von organisatorischen oder technischen Schutzfunktionen für die Umsetzung in der Organisation.
- Durchführen (Do): Umsetzen und Betreiben des ISMS, also Sicherheitsmaßnahmen realisieren, für ihre Einhaltung sorgen und Informationssicherheit im laufenden Betrieb inklusive in Notfällen bzw. bei Krisen gewährleisten. In dieser Phase findet die Realisierung der Schutzfunktionen

(organisatorisch, technisch) statt. Darüber hinaus wird ein Monitoring anhand von festgelegten Kennzahlen für das betriebene ISMS in diesem Abschnitt etabliert. Auch die Abwicklung von Awareness-Trainings findet in dieser Phase statt. Für einen späteren Vergleich (siehe nächste Phase) werden auch Daten zu (Sicherheits-)Kennzahlen gemessen. Dadurch wird die Grundlage für die spätere kontinuierliche Verbesserung des ISMS gelegt. Für die Vergleiche werden die Zielvorgaben herangezogen.

- Prüfen (Check): Überwachen und Überprüfen des ISMS auf seine Wirksamkeit, also Vorhandensein, Sinnhaftigkeit, Einhaltung der Sicherheitsmaßnahmen überprüfen, aber auch Kenntnis über Vorfälle sowie üblicher Good-Practices erlangen. Das bedeutet sowohl eine Validierung („wird das richtige ISMS entwickelt/betrieben?“) als auch eine Verifikation („wird das ISMS richtig entwickelt/betrieben?“) sind Gegenstand dieser Check-Phase zur Überprüfung des ISMS. Realisierbar ist dies unter Abwicklung von Audits (z.B. intern, extern) oder durch Tests wodurch die Anwesenheit von Fehlern (die anschließend behebbar sind) zeigbar ist. Regelmäßige Übungen oder Tests wie etwa im Bereich der Business Continuity oder im Bereich der Notfallvorsorge sind ebenso Gegenstand dieser Phase wie Security-Assessments die sich sowohl auf die Organisation, auf die Produkte bzw. Dienstleistungen aber auch auf das ISMS beziehen können. Die Beobachtungen bzw. die Messwerte sind ausreichend zu dokumentieren und anhand von Vergleichen mit den Zielwerten ist die nächste Phase zur Verbesserung einzuleiten.
- Handeln (Act): Instandhalten und Verbessern des ISMS, das bedeutet auf erkannte Fehler, Schwachstellen und veränderte Umfeldbedingungen reagieren und die Ursachen für Gefährdungen beseitigen. Dies bedingt erneutes Planen, womit sich ein ständiger Kreislauf schließt. Der Schwerpunkt dieser Phase liegt demzufolge in der laufenden also in der kontinuierlichen Optimierung des ISMS. Vordergründig sich ändernde Rahmenparameter und die in den vorherigen Phasen gemachten Beobachtungen sollten hier berücksichtigt werden. Verändern kann sich etwa auch die Rechtslage durch Aktualisierungen von Rechtsgrundlagen.

Aufbau eines ISMS

Abbildung 1.3: Wesentliche Prozessschritte zur Umsetzung und Verwendung eines ISMS

In Verbindung mit einem ISMS wie das etwa in Anlehnung an die Standards ISO/IEC 27001 Annex A iVm ISO 27002 sowie gem. BSI IT-Grundschutz entwickelt, betrieben und adaptiert wird stellt sich auch die Frage, wie ein solches ISMS auf der Basis des PDCA-Cycle in vereinfachter und zusammengefasster Form aufgebaut werden kann. Es lassen sich für die Realisierung eines ISMS fünf konsolidierte Phasen zusammenfassen, wie in der Abbildung dargestellt.

1. **Scope definieren.** Für die Umsetzung eines ISMS gem. ISO/IEC 27001 ist eine Einschränkung der anwendbaren Organisationsbestandteile (z.B. Aufbau- und Ablauforganisation, Abteilungen, Referate, Bereiche, Sektionen) möglich. Das bedeutet festzulegen welche Organisationseinheiten vom ISMS unter ISO/IEC 27001 betroffen sind. Dabei kann es sich um verschiedene Abteilungen (organisatorisch) oder unterschiedliche physische Standorte („örtlich“) oder aber etwa auch um ausgewählte technische Systeme für die Erbringung von kritischen Geschäftsprozessen („Technisch“) handeln.
2. **Assets & Schutzbedarf.** Die Identifizierung der zu schützenden Assets – dabei ist generell eine Unterscheidung zwischen primären Assets (z.B. zu schützende Daten wie Akte, Verträge, Personaldaten, Geschäftsgeheimnisse) und sekundären Assets durchführbar (z.B. kryptografisches Schlüsselmaterial zum Schutz der primären Assets) – bietet die Grundlage für eine Schutzbedarfsanalyse. Bei der Auswahl zu schützender Assets sowie bei der Ableitung des Schutzbedarfs können eine Vielzahl möglicher Aspekte berücksichtigt werden. Darunter sind zusammengefasst etwa relevante Hardware (z.B. Datenbanksysteme, Server, Speicher), erforderliche Software (z.B. Source Code), Applikationen (z.B. Intranet, Webapplikationen, lauffähiger Source Code), essenzielle Daten (z.B. Bestellmengen, Kontaktlisten zur Notfallvorsorge), allgemeine Prozesse bzw. insbesondere Geschäftsprozesse (z.B. kritische Kernprozesse oder relevante Unterstützungsprozesse), die wichtigsten Produkte (z.B. damit verbundene Geschäftsgeheimnisse) oder beispielsweise die rentabelsten Dienstleistungen (z.B. digitale Services).
3. **Risiko-Management.** In Verbindung mit den zuvor genannten identifizierten Assets wird im Rahmen des Risikomanagements eine Auflistung bzw. eine konsolidierte Sammlung der Assets (auch bezeichnet als: „Asset Inventory“) erstellt. Im Fokus steht die Risiko-Behandlung, um die durch Angreifer vorhandenen Bedrohungen auf Assets und die daraus entstehenden Risiken zu behandeln. Nämlich, um entweder die Eintrittswahrscheinlichkeit eines Risikos zu reduzieren oder die damit verbundenen Auswirkungen, sofern sich das betreffende Risiko materialisiert, abzuschwächen. Auch sind andere Maßnahmen denkbar, wie Vermeidung von Risiken oder die Auslagerung ausgewählter Geschäftsprozesse bzw. technischer Systeme. Demzufolge ist die Betrachtung von Angreifern (z.B. intern oder extern) und die Untersuchung möglicher Angriffsszenarien welche sich auf die identifizierten Assets auswirken. Im Rahmen des Risikomanagements ist auch die Behandlung von Maßnahmen in der Form denkbar, um die Auswirkungen von (zumeist erfolgreichen) Angriffen zu reduzieren. Gemeinsam mit den erkannten Risiken ist zur Erkennung von

Lücken bei Sicherheitsmaßnahmen gem. ISO/IEC 27001 ein Gap-Assessment durchführbar, um den aktuellen Status der Umsetzung in der Organisation (z.B. Amt, Behörde, Institution, Unternehmen) zu eruieren. Das Gap-Assessment wird für alle relevanten Referenzmaßnahmenziele abgewickelt (z.B. A.5 bis A.18) Im nächsten Schritt können darauf aufbauend Maßnahmen realisiert werden.

4. **Maßnahmen umsetzen.** Die getroffenen Maßnahmen können entweder isoliert betrachtet unter Berücksichtigung der ISO/IEC 27001 Annex A sowie in Verbindung mit der ISO/IEC 27002 umgesetzt werden. Die ISO/IEC 27002 trägt durch Umsetzungsrichtlinien zur Orientierung bei der Realisierung der in Annex A beschriebenen Schutzfunktionen im Hinblick auf die Informationssicherheit bei. Auch Erweiterungen der ISO/IEC 27001 sind etwa durch datenschutzrelevante ISO-Standards (z.B. 27701) möglich, um Kriterien im Hinblick auf den Datenschutz im Organisationsumfeld verstärkt zu implementieren. Darüber hinaus kann die ergänzende Berücksichtigung ausgewählter Aspekte aus dem IT-Grundschutz hilfreich sein.
5. **Kontinuierliche Verbesserung.** Durch den kontinuierlichen Verbesserungsprozess (auch: „KVP-Modell“) ist eine regelmäßige Auseinandersetzung mit dem ISMS gegeben. Das bedeutet, dieses KVP-Modell sorgt bei korrekter Anwendung dafür, dass einerseits das ISMS selbst einer ständigen Evaluation und demzufolge einer regelmäßigen Optimierung unterliegt. Andererseits sorgt dieses KVP-Modell auch dafür, dass die durch das ISMS realisierten Schutzfunktionen (z.B. organisatorisch, technisch) ebenso einer ständigen Prüfung unterliegen und bei Bedarf eine Verbesserung eingeleitet wird. Neben der kontinuierlichen Optimierung bietet sich auch etwa in Anlassfällen eine Einleitung von Verbesserungsmaßnahmen an (sog. „ad-hoc“).

Gap-Assessment

In einem Gap-Assessment erfolgt die Identifizierung von Lücken in der Umsetzung von Schutzfunktionen zur Erreichung von Sicherheitszielen für die Informationssicherheit im Hinblick auf damit verbundene Standards (z.B. BSI IT-Grundschutz, ISO/IEC 27001). Es lassen sich vier Prozessschritte ableiten:

Abbildung 1.4: Die vier Prozessschritte zur Erstellung eines Gap-Assessments

1. **Identifizieren des aktuellen Status.** Für eine Behörde, Institution oder für ein Unternehmen wird für den Anwendungsbereich der aktuelle Zustand der umgesetzten Schutzfunktionen eruiert. Dabei werden die im Anwendungsbereich festgelegten Abteilungen, Fachbereiche, Standorte oder Prozesse und auch IT-Systeme evaluiert. Berücksichtigt wird der Lebenszyklus sowohl der Daten als auch der verwendeten Systeme. Zu Beginn erfolgt die Identifizierung eines allgemeinen Sicherheitsniveaus im Anwendungsbereich. Das bedeutet, die Aufbau- bzw. die Ablauforganisation wird im Hinblick auf die referenzierten Kriterien (z.B. die Referenzmaßnahmenziele der ISO/IEC 27001 wie etwa A.5 bis A.18). Dieser Schritt umfasst auch die Evaluierung der generellen Ausstattung (z.B. verwendete Büro-Computer). Im nächsten Schritt erfolgt die Evaluierung der Herstellung (z.B. Architektur, Design, Entwicklung) der durch die Organisation, die Institution oder durch das Unternehmen erbrachten Dienstleistungen oder für die hergestellten Produkte. Damit wird das Sicherheitsniveau der Produkterstellung geprüft. Anschließend wird die Herstellung (z.B. in großen Stückzahlen, aber auch etwa bei Los-Größe 1) der zuvor erwähnten Produkte oder der Dienstleistungen auf Lücken untersucht. Nach der Herstellung wird der Schwerpunkt auf Sicherheitstests – auch dies betrifft sowohl Tests für organisatorische Aspekte (z.B. Business Continuity-Tests) als auch im Hinblick auf lauffähige Programme oder etwa bereitgestellte bzw. genützte IT-Systeme. Liefert die Organisation Produkte, Daten oder Informationen an Dritte (z.B. natürliche oder juristische Personen) erfolgt in diesem Bereich der nächste Schritt für das Gap-Assessment.
2. **Ableiten des Zielzustands.** Für die Organisation und durch die Organisation verwaltete bzw. bereitgestellte Assets wird in diesem Schritt ein Zielzustand abgeleitet. Dabei ist der gesamte Lebenszyklus von Produkten, der Organisation selbst und auch von Daten zu berücksichtigen. Der Zielzustand wird wieder auf die ISMS-Kontrollgruppen (für ISO/IEC 27001 Annex A iVm ISO/IEC 27002 etwa A-15 bis A-18) abgebildet.
3. **Durchführen einer Risikoanalyse.** Eine vollständige Risikoanalyse stellt die Grundlage für ein Gap-Assessment dar. Dies ist im Rahmen des Risikomanagementprozesses abzuwickeln. Dazu werden vor dem Hintergrund von Angriffsszenarien Risiken identifiziert und ferner ein Risikobehandlungsplan abgeleitet. Auch Aspekte der Geschäftskontinuität („Business Continuity“) etwa zur Adressierung von Notfällen, Krisen oder vergleichbaren Szenarien sollten an dieser Stelle berücksichtigt werden.
4. **Schließen der Lücken.** In diesem Schritt wird auf der Grundlage dieser Risikoanalyse eine Auswahl der relevanten Risikobehandlungsmaßnahmen durchgeführt. Eine Nachverfolgung der Umsetzung von Sicherheitsmaßnahmen soll gewährleisten, dass die erkannten Lücken geschlossen werden.

Am Beginn stehen Sicherheitsziele, also Erwartungen und Anforderungen der Verantwortlichen und Beteiligten. Durch die Planungs-, Durchführungs-, Prüf- und Verbesserungsprozesse bzw. -handlungen werden sie erfüllt - das schließlich akzeptierte Sicherheitsniveau wird erreicht.

Informationssicherheitsmanagement ist also ein kontinuierlicher Prozess. In den folgenden Kapiteln wird dargestellt, welche Aufgaben eines ISMS umgesetzt und welche Sicherheitsmaßnahmen implementiert werden können zur:

- Festlegung der Sicherheitsziele und -strategien der Organisation,
- Ermittlung und Bewertung der Informationssicherheitsrisiken (information security risk assessment),
- Festlegung geeigneter Sicherheitsmaßnahmen,
- Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Maßnahmen,
- Förderung des Sicherheitsbewusstseins innerhalb der Organisation sowie
- Entdeckung von und Reaktion auf sicherheitsrelevante Ereignisse (information security incident handling).

1.3 Orientierung im Informationssicherheitshandbuch

Aufgrund seines Bestrebens das Thema Informationssicherheit mit all seinen Aspekten und Elementen möglichst vollständig zu behandeln, weist das österreichische Sicherheitshandbuch einen beträchtlichen Umfang auf. Eine vollständige Lektüre des Sicherheitshandbuchs mit all seinen Kapiteln und Anhängen wird damit zunehmend zur Herausforderung. Zudem wird es aufgrund des stetig wachsenden Umfangs immer schwieriger, die für die eigene Zielgruppe speziell relevanten Inhalte zu identifizieren. Um hier gegenzusteuern, gibt dieser Abschnitt einen Überblick über die Struktur des Sicherheitshandbuchs, erleichtert die Orientierung und Navigation durch dessen Inhalte und bietet zielgruppenspezifische Vorschläge zum effizienten Auffinden besonders relevanter Inhalte.

1.3.1 Herausforderungen in der Lektüre des Sicherheitshandbuchs

Das österreichische Sicherheitshandbuch nähert sich dem Thema Informationssicherheit über das Konzept eines sogenannten Informationssicherheitsmanagementsystems (ISMS), welches innerhalb einer Organisation einen systematischen Umgang mit relevanten Aspekten der Informationssicherheit gewährleistet. Dementsprechend orientiert sich auch die

Struktur des Sicherheitshandbuchs primär an jener der Normen ISO/IEC 27001 und ISO/IEC 27002, welche Planung, Umsetzung, Betrieb und laufende Verbesserung eines ISMS definieren, sowie konkrete Vorgaben zur Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen geben.

Die Anlehnung der Struktur des Sicherheitshandbuchs an jene eines etablierten und weit verbreiteten Standards ist sinnvoll, da der Aufbau solcher Standards in der Regel wohlüberlegt und auch einem laufenden Aktualisierungs- und Optimierungsprozess unterworfen ist. Allerdings bringt die Übernahme der Struktur der erwähnten ISO/IEC-Standards auch einige Nachteile mit sich. So scheint bereits der Aufbau der Norm ISO/IEC 27001 speziell für mit der Materie nicht so vertraute Personen zunächst oft wenig intuitiv und nachvollziehbar. Die Eleganz und Sinnhaftigkeit des Aufbaus erschließen sich somit oft erst zu einem späteren Zeitpunkt, wenn ein tieferes Verständnis der im Standard definierten Konzepte und Ansätze erarbeitet wurde. Umgelegt auf das Sicherhandbuch bedeutet dies, dass Leserinnen und Leser mit wenig Vorwissen zu Informationssicherheitsmanagementsystemen vor allem zu Beginn Probleme haben können, sich im Sicherheitshandbuch zu orientieren. Ein weiteres Problem kann sich daraus ergeben, dass das Sicherheitshandbuch das Thema Informationssicherheit möglichst breit und vollständig betrachtet, sich also bewusst an unterschiedliche Zielgruppen richtet. Während einige Themen unabhängig von der Zielgruppe immer von Bedeutung sind, können andere Themen je nach Zielgruppe durchaus eine unterschiedliche Relevanz aufweisen. So werden Aspekte der Disaster Recovery und Business Continuity speziell für größere Organisationen von Bedeutung sein, für Privatpersonen jedoch eher eine untergeordnete Rolle spielen. Da sich das Sicherheitshandbuch an unterschiedlichste Zielgruppen wendet, enthält dieses auch Themen, die nicht notwendigerweise für alle Leserinnen und Leser gleich relevant und interessant sind. Das Identifizieren der für die eigene Zielgruppe relevanten Inhalte kann dadurch zur Herausforderung werden.

Um diese Probleme zu adressieren und die damit verbundenen Herausforderung zu meistern, stellt der folgende Abschnitt zunächst die Struktur des Sicherheitshandbuchs näher vor. Im nachfolgenden Abschnitt wird dann anhand von vier exemplarischen Zielgruppen ((1) Privatpersonen, (2) Ein-Personen-Unternehmen (EPU), (3) Klein- und Mittelbetriebe (KMU) und (4) Großunternehmen und Behörden) die Relevanz der einzelnen Kapitel und Anhänge des Sicherheitshandbuchs gewichtet, um so ein zielgerichteteres Auffinden der für die jeweilige Zielgruppe speziell relevanten Themenbereiche zu unterstützen.

1.3.2 Aufbau des Sicherheitshandbuchs

Entsprechend seinem Bestreben sich dem Thema Informationssicherheit über das Konzept des Informationssicherheitsmanagements zu nähern, folgt der Aufbau des Sicherheitshandbuchs weitgehend der Struktur der Normen ISO/IEC 27001 und ISO/IEC 27002. Konkret setzt sich der Hauptteil des österreichischen Sicherheitshandbuchs aus den folgenden Abschnitten zusammen:

- **1 Einführung.** Dieses erste Kapitel des Sicherheitshandbuchs enthält allgemeine Informationen und Einführungen zum Sicherheitshandbuch selbst und gibt einen ersten Überblick über Konzepte und Ziele des Informationssicherheitsmanagements.
- **2 Informationssicherheitsmanagementsystem (ISMS).** Dieses Kapitel beschreibt im Detail die Ziele und Konzepte eines Informationssicherheitsmanagementsystems (ISMS).
- **3 Managementverantwortung und Aufgaben beim ISMS.** Dieses Kapitel geht im Detail auf die Aufgaben des Managements eines Unternehmens im Rahmen eines ISMS ein.
- **4 Informationssicherheitspolitik.** Dieses Kapitel widmet sich der Erstellung und laufenden Wartung einer unternehmensweiten Informationssicherheitspolitik (Security Policy), welche die grundlegenden Ziele und Verhaltensweisen in Bezug auf Informationssicherheit innerhalb eines Unternehmens vorgibt.
- **5 Risikomanagement.** Dieses Kapitel beschreibt Ansätze und Methoden der Risikoanalyse und die weitere Behandlung der identifizierten Risiken. Die Durchführung einer Risikoanalyse ist fundamental, um eigene Vermögenswerte (Assets) und deren Bedrohungen zu identifizieren und um basierend darauf geeignete Sicherheitsmaßnahmen treffen zu können.
- **6 Organisation.** Dieses Kapitel widmet sich der Frage, über welche organisatorischen Prozesse der effektive Betrieb eines ISMS in einem Unternehmen unterstützt werden kann.
- **7 Personelle Sicherheit.** Dieses Kapitel des Sicherheitshandbuchs widmet sich Aspekten der personellen Sicherheit innerhalb eines Unternehmens, wie z.B. der Definition und Umsetzung von Regeln für Mitarbeiterinnen und Mitarbeiter.
- **8 Vermögenswerte und Klassifizierung von Informationen.** Dieses Kapitel widmet sich der Identifikation von Vermögenswerten (Assets) und der Bewertung ihrer Kritikalität und ihres Schutzbedarfs. Damit steht dieses Kapitel in engem Zusammenhang mit Kapitel 4 (Risikoanalyse), da die Erfassung von Vermögenswerten eine Grundvoraussetzung für die Durchführung einer Risikoanalyse ist.
- **9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung.** Dieses Kapitel adressiert die Kontrolle und Beschränkung des Zugriffs auf IT-Systeme. Dabei handelt es sich um eine für die Informationssicherheit zentrale Sicherheitsfunktion, deren diversen Aspekte in diesem Kapitel näher erörtert werden.

- **10 Kryptographie.** Dieses Kapitel widmet sich dem Einsatz kryptographischer Methoden und den in diesem Zusammenhang zu beachtenden Aspekten. Es beschreibt einerseits grundlegende kryptographische Methoden und erörtert andererseits wichtige Aspekte bezüglich ihres praktischen Einsatzes.
- **11 Physische und umgebungsbezogene Sicherheit.** Dieses Kapitel adressiert Themen der physischen und umgebungsbezogenen Sicherheit. Es geht im Speziellen auf Aspekte der Raum- und Gebäudesicherheit wie bauliche Maßnahmen, Brandschutz, Leitungsführung oder auch Stromversorgung ein.
- **12 Sicherheitsmanagement im Betrieb.** Dieses Kapitel des Sicherheitshandbuchs widmet sich speziell den relevanten Aspekten des Betriebs eines Informationssicherheitsmanagementsystems (ISMS). Dazu gehören die Erstellung und Wartung von Dokumentationen, Erstellung von Sicherheits- und Datensicherungskonzepten, oder auch die Durchführung laufender Protokollierungen und Monitorings.
- **13 Sicherheitsmanagement in der Kommunikation.** Dieses Kapitel beschreibt einerseits Aspekte der Netzwerksicherheit und andererseits Themen im Zusammenhang mit dem sicheren elektronischen Austausch von Daten.
- **14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems.** Dieses Kapitel des Sicherheitshandbuchs beschreibt relevante Aspekte bezüglich Entwicklung, Betrieb und Wartung von IT-Systemen.
- **15 Lieferantenbeziehungen.** Dieses Kapitel widmet sich Sicherheitsaspekten im Zusammenhang mit der Interaktion mit Lieferanten.
- **16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling).** Dieses Kapitel beschreibt notwendige Prozesse zum geeigneten Umgang mit Informationssicherheitsereignissen.
- **17 Disaster Recovery und Business Continuity.** Dieses Kapitel des Sicherheitshandbuchs beschreibt notwendige Prozesse für ein betriebliches Kontinuitätsmanagement inklusive der definierten und zeitnahen Rückkehr in den Normalbetrieb nach unvorhergesehenen Ausfällen.
- **18 Security Compliance.** Dieses Kapitel definiert notwendige Überprüfungen der Einhaltung geltender Vorgaben und das laufende Monitoring der Informationssicherheit.

Darüber hinaus enthält das Sicherheitshandbuch noch diverse Anhänge, die sich jeweils einem bestimmten Aspekt der Informationssicherheit im Detail widmen:

- **A.1 Sicherheitsszenarien.** Dieser Anhang des Sicherheitshandbuchs widmet sich Themen der industriellen Sicherheit und des E-Governments in Österreich.
- **A.2 Sicherheitstechnologien.** Dieser Anhang beschreibt ausgewählte Sicherheitstechnologien.
- **A.3 Cloud Computing.** Dieser Anhang diskutiert sicherheitsrelevante Aspekte aus dem Bereich Cloud Computing.
- **A.4 Smartphone Sicherheit.** Dieser Anhang des Sicherheitshandbuchs widmet sich dem Thema Smartphone-Sicherheit.

- **A.5 Sicherheit in sozialen Netzen.** Dieser Anhang des Sicherheitshandbuchs beschreibt sicherheitsrelevante Aspekte, die im Zusammenhang mit der Verwendung sozialer Netze beachtet werden müssen.
- **A.6 Sichere Beschaffung.** Dieser Anhang geht auf diverse Aspekte der Informationssicherheit im Rahmen von Beschaffungsvorgängen näher ein und definiert hierfür ein relativ formales und prozessgetriebenes Vorgehen.

Vervollständigt wird das Sicherheitshandbuch schließlich von weiteren Anhängen, die hauptsächlich ergänzendes Material bereitstellen bzw. Verweise zu externen Informationsquellen bieten:

- **B Muster für Verträge, Verpflichtungserklärungen und Dokumentationen.** Dieser Anhang enthält Vorlagen für diverse Dokumente aus dem Bereich ISMS und Informationssicherheit.
- **C.1 Wichtige Normen.** Dieser Anhang enthält eine Liste relevanter Normen und Standards aus dem Bereich ISMS und Informationssicherheit.
- **C.2 Referenzdokumente.** Dieser Anhang listet Dokumente, auf die im Sicherheitshandbuch direkt Bezug genommen wird.
- **D Referenztabellen.** Dieser Anhang enthält eine tabellarische Gegenüberstellung der Strukturen der Versionen 3.1.5 und 4 des Sicherheitshandbuchs.
- **E Referenzierte IKT-Board-Beschlüsse und Gesetze.** Dieser Anhang enthält eine Liste der im Sicherheitshandbuch referenzierten IKT-Board-Beschlüsse und Gesetze.
- **F Wichtige Adressen.** Dieser Anhang enthält Adressen von Organisationen, die mit dem Sicherheitshandbuch in Zusammenhang stehen.

1.3.3 Zielgruppenspezifische Leitfäden

Alle im österreichischen Sicherheitshandbuch abgedeckten Themenbereiche sind relevant in Bezug auf Informationssicherheit. Allerdings sind nicht alle Themen für alle Zielgruppen gleichermaßen wichtig. So werden vor allem in Bezug auf organisatorische Sicherheitsmaßnahmen für Unternehmen mit mehreren tausend Mitarbeitern (z.B. sog. „Großunternehmen“) andere Aspekte von Bedeutung sein als für Ein-Personen-Unternehmen (EPU), Klein- und Mittelbetriebe (KMU) oder gar Privatpersonen.

Die Lektüre des gesamten Sicherheitshandbuchs stellt für alle Zielgruppen immer den Idealfall dar – ein Idealfall, der in der Praxis ob des Umfangs des Sicherheitshandbuchs wohl nur selten Anwendung finden wird. Realitätsnäher sind wohl Szenarien, in denen Leserinnen und Leser des Sicherheitshandbuchs einzelne Abschnitte und Themenbereiche gezielt auswählen. Die Herausforderung liegt dabei in der geeigneten Wahl der für die eigene Zielgruppe relevanten Passagen. Dieser Abschnitt soll bei dieser Wahl unterstützen. Dazu wird in diesem Abschnitt

für ausgewählte exemplarische Zielgruppen die Relevanz der einzelnen Kapitel und technischen Anhänge des Sicherheitshandbuchs bewertet. Dadurch ergibt sich für jede Zielgruppe ein Vorschlag, in welcher Reihenfolge die einzelnen Kapitel des Sicherheitshandbuchs konsumiert werden können.

Hinweis: Die für die exemplarischen Zielgruppen vorgenommenen Bewertungen und Reihungen der einzelnen Abschnitte und Themenbereiche des Sicherheitshandbuchs sind ausschließlich zur besseren Orientierung gedacht. Keinesfalls soll der Eindruck entstehen, dass weiter hinten gereihte Themen für die jeweilige Zielgruppe keine Relevanz haben. Im Gegenteil, Informationssicherheit kann nur gewährleistet sein, wenn diese in all ihren Aspekten ganzheitlich betrachtet und umgesetzt wird. Die vorgeschlagene Reihung soll es jedoch ermöglichen, sich mit den für die eigene Zielgruppe besonders wichtigen Themen zuerst zu befassen, um so aus dem Sicherheitshandbuch schnellstmöglich den größtmöglichen persönlichen Nutzen ziehen zu können.

1.3.3.1 Zusammenfassender Überblick

In den nachfolgenden Unterabschnitten wird die Relevanz der einzelnen Kapitel des Sicherheitshandbuchs anhand von vier exemplarischen Zielgruppen beschrieben und argumentiert. Zuvor zeigt dieser Unterabschnitt anhand der folgenden Tabelle einen zusammenfassenden Überblick. Die untenstehende Tabelle verwendet zur Verdeutlichung der Relevanz der einzelnen Kapitel für die vier ausgewählten Zielgruppen sowie für eine abschließende Gesamteinstufung (A ist höher priorisierbar als H) des Sicherheitshandbuchs ein einheitliches Farbschema. Aus der tabellarischen Übersicht wird ersichtlich, dass mit zunehmender Organisationsgröße die einzelnen Kapitel des Sicherheitshandbuchs stetig an Bedeutung gewinnen. Dies ist insofern nachvollziehbar, als dass das Sicherheitshandbuch sich dem Thema Informationssicherheit über ein ISMS nähert. Während ein solches kleinere Unternehmen und Privatpersonen in vielen Fällen mit seinem eigenen Formalismus vor schwer zu bewältigende Herausforderungen stellt, ist ein ISMS mit zunehmender Unternehmensgröße in der Regel notwendig.

	Kapitel	Privat-Personen	EPU	KMU	Großunternehmen und Behörden	Gesamt
	1 Einführung	hoch	hoch	hoch	hoch	A
Aufbau & Risikoanalyse	2 Informationssicherheitsmanagementsystem (ISMS)	gering	gering	mittel	hoch	G
	3 Managementverantwortung und Aufgaben beim ISMS	gering	gering	mittel	hoch	G
	4 Risikoanalyse	mittel	hoch	hoch	hoch	B
	5 Informationssicherheitspolitik	gering	mittel	mittel	hoch	F
Umsetzung & Maßnahmen	6 Organisation	gering	mittel	mittel	hoch	F
	7 Personelle Sicherheit	gering	gering	mittel	hoch	G
	8 Vermögenswerte und Klassifizierung von Informationen	mittel	hoch	hoch	hoch	B
	9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung	hoch	hoch	hoch	hoch	A
	10 Kryptographie	mittel	hoch	hoch	hoch	B
	11 Physische und Umgebungsbezogene Sicherheit	mittel	mittel	hoch	hoch	C
	12 Sicherheitsmanagement im Betrieb	gering	mittel	mittel	hoch	F
	13 Sicherheitsmanagement in der Kommunikation	mittel	hoch	hoch	hoch	B
	14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems	mittel	hoch	hoch	hoch	B
	15 Lieferantenbeziehungen	gering	hoch	hoch	hoch	E
Betrieb & Reaktion	16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)	mittel	mittel	mittel	hoch	D
	17 Disaster Recovery und Business Continuity	mittel	mittel	mittel	hoch	D
	18 Security Compliance	gering	gering	mittel	hoch	G
Technologie-trends	A.1 Sicherheitsszenarien	gering	gering	gering	hoch	H
	A.2 Sicherheitstechnologien	mittel	mittel	mittel	hoch	D
	A.3 Cloud Computing	hoch	hoch	hoch	hoch	A
	A.4 Smartphone Sicherheit	hoch	hoch	hoch	hoch	A
	A.5 Sicherheit in Sozialen Netzwerken	hoch	hoch	hoch	hoch	A
	A.6 Sichere Beschaffung	mittel	mittel	mittel	hoch	D

Darstellung: sicherheitshandbuch.gv.at

hoch mittel gering

Abbildung 1.5: Zusammenfassung vorgeschlagener Priorisierung der Inhalte im Sicherheitshandbuch

An dieser Stelle sei nochmal darauf hingewiesen, dass die vorgenommene Bewertung der Relevanz für unterschiedliche Zielgruppen sowie die angegebene Gesamteinstufung als vorgeschlagener Richtwert zu verstehen ist, der nicht notwendigerweise auch auf jeden Einzelfall zutrifft. Die Grundlage für diese Einstufung sind Erfahrungswerte. In diesem Zusammenhang ist auch zu beachten, dass eine über die Farbe Rot angedeutete geringe Relevanz eines Themas für eine Zielgruppe nicht bedeutet, dass diese Zielgruppe dieses Thema komplett ignorieren darf. Das bedeutet auch in Abhängigkeit sicherheitskritischer Aspekte wie Kritikalität zu verarbeitender Daten oder dem jeweiligen Wert von Assets sind Verschiebungen oder Veränderungen der jeweiligen Relevanz in allen Zielgruppen bzw. der Gesamteinstufung möglich. Die Kategorisierung der Relevanz soll dabei unterstützen, bei beschränkten zeitlichen Ressourcen eine passende Priorisierung der einzelnen Kapitel zu finden. Die vollständige Lektüre des Sicherheitshandbuchs stellt in jedem Fall den erstrebenswerten Idealfall dar.

Der folgenden Abschnitte gehen auf die Details zur jeweiligen zielgruppenspezifischen Relevanz der Kapitel im Sicherheitshandbuch ein, die der Ableitung der oben angegebenen zusammenfassenden Tabelle zugrunde liegen. Die Gesamteinstufung wurde aus den einzelnen Werten für die vier Zielgruppen abgeleitet und basiert auf Erfahrungswerten.

1.3.3.2 Zielgruppe: Privatpersonen

Mit seinem Ansatz, sich dem Thema Informationssicherheit über das Konzept eines Informationssicherheitsmanagementsystems (ISMS) zu nähern, richtet sich das österreichische Sicherheitshandbuch implizit primär an Unternehmen unterschiedlicher Größe. Ungeachtet dessen behandelt das Sicherheitshandbuch Themenbereiche, die auch für Privatpersonen von Interesse sein können. In diesem Abschnitt wird daher die Relevanz der einzelnen Kapitel des Sicherheitshandbuchs aus der Sicht von Privatpersonen bewertet. Die Bewertung erfolgt über eine dreistufige Farbskala. Grün symbolisiert, dass das betreffende Kapitel und das darin behandelte Themengebiet für Privatpersonen besonders relevant sind. Orange zeigt an, dass das betreffende Kapitel durchaus auch für Privatpersonen relevante und interessante Inhalte umfasst, jedoch potenziell nicht alle Vorgaben aus dem Kapitel von Bedeutung sind. Rot markiert sind schließlich jene Kapitel des Sicherheitshandbuchs, die für Privatpersonen nur eine untergeordnete Rolle spielen, da sie sich primär an Unternehmen richten.

1 Einführung
Dieses erste Kapitel des Sicherheitshandbuchs enthält allgemeine Informationen und Einführungen, die sich an alle Zielgruppen richten. Damit ist dieses Kapitel auch für Privatpersonen relevant.

2 Informationssicherheitsmanagementsystem (ISMS)
Dieses Kapitel beschreibt Konzepte eines Informationssicherheitsmanagementsystems (ISMS). Die Etablierung und der Betrieb eines ISMS ist für Privatpersonen wenig realistisch und sinnvoll. Dieses Kapitel spielt für diese daher nur eine untergeordnete Rolle.

3 Managementverantwortung und Aufgaben beim ISMS
Dieses Kapitel beschreibt im Detail die Aufgaben des Managements im Rahmen eines ISMS. Da Managementstrukturen ausschließlich für Unternehmen relevant sind, ist keine Relevanz dieses Kapitels für Privatpersonen gegeben.

4 Informationssicherheitspolitik

Dieses Kapitel widmet sich der Erstellung und laufenden Wartung einer unternehmensweiten Informationssicherheitspolitik (Security Policy). Auch wenn einzelne Elemente wie etwa die Definition des eigenen Zugangs zum Thema Informationssicherheit und der damit verbundenen Erwartungshaltungen und Ziele auch für Privatpersonen bis zu einem gewissen Grad sinnvoll sein können, richten sich die Inhalte dieses Kapitels doch primär an Unternehmen und sind für Privatpersonen insgesamt wenig relevant.

5 Risikomanagement

Dieses Kapitel beschreibt Ansätze und Methoden der Risikoanalyse und die weitere Behandlung der identifizierten Risiken. Die Durchführung einer Risikoanalyse ist fundamental, um eigene Vermögenswerte (Assets) und deren Bedrohungen zu identifizieren und um basierend darauf geeignete Sicherheitsmaßnahmen treffen zu können. Auch wenn formale Methoden der Risikoanalyse für Privatpersonen zu weit gehen würden, ist das prinzipielle Bewusstsein über eigene Vermögenswerte und deren potenzielle Bedrohungen auch im privaten Umfeld hilfreich. Dieses Kapitel des Sicherheitshandbuchs kann hierbei unterstützen und nützliche Denkanstöße geben.

6 Organisation

Dieses Kapitel widmet sich vor allem der Frage, über welche organisatorischen Prozesse der effektive Betrieb eines ISMS in einem Unternehmen unterstützt wird. Für Privatpersonen ist dieses Kapitel damit wenig relevant.

7 Personelle Sicherheit

Dieses Kapitel des Sicherheitshandbuchs widmet sich Aspekten der personellen Sicherheit, wie z.B. der Definition und Umsetzung von Regeln für Mitarbeiterinnen und Mitarbeiter. Für Privatpersonen ist dieser Abschnitt damit wenig relevant, auch wenn einzelne in diesem Abschnitt behandelte Sicherheitsaspekte – wie z.B. Clear-Desk-Policy – auch im privaten Umfeld hilfreich sein können.

8 Vermögenswerte und Klassifizierung von Informationen

Dieses Kapitel widmet sich der Identifikation von Vermögenswerten (Assets) und der Bewertung ihrer Kritikalität und ihres Schutzbedarfs. Damit steht dieses Kapitel in engem Zusammenhang mit Kapitel 4 (Risikoanalyse), da die Erfassung von Vermögenswerten eine Grundvoraussetzung für die Durchführung einer Risikoanalyse ist. Auch wenn Privatpersonen in der Regel kaum formale Risikoanalysen durchführen werden, ist das prinzipiell Bewusstsein um Vermögenswerte und die damit zusammenhängenden Bedrohungen auch für Privatpersonen sinnvoll.

9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung

Dieses Kapitel adressiert die Kontrolle und Beschränkung des Zugriffs auf IT-Systeme. Dabei handelt es sich um eine für die Informationssicherheit zentrale Sicherheitsfunktion. Die Relevanz ist auch für Privatpersonen gegeben, da auch diese ihre Daten und privaten IT-Systeme in der Regel über entsprechende Zugriffskontrollsysteme absichern.

10 Kryptographie

Dieses Kapitel widmet sich dem Einsatz kryptographischer Methoden und den in diesem Zusammenhang zu beachtenden Aspekten. Kryptographische Methoden und die darauf aufbauenden Lösungen und Produkte sind das Fundament der Informationssicherheit. Die Kenntnis ihrer Möglichkeiten und Limitierungen kann daher auch für Privatpersonen bis zu einem gewissen Grad interessant sein.

11 Physische und umgebungsbezogene Sicherheit

Dieses Kapitel adressiert Themen der physischen und umgebungsbezogenen Sicherheit und geht im Speziellen auf Aspekte der Raum- und Gebäudesicherheit ein. Diese Themen sind speziell relevant für größere Unternehmen, die über umfangreiche Betriebsstätten (Bürogebäude, Serverräume, Rechenzentren, etc.) verfügen. Für Privatpersonen ist die Relevanz damit nur bedingt gegeben, wobei einzelne Aspekte der Raum- und Gebäudesicherheit auch für diese interessant sein können.

12 Sicherheitsmanagement im Betrieb

Dieses Kapitel des Sicherheitshandbuchs widmet sich relevanten Aspekten des Betriebs eines Informationssicherheitsmanagementsystems (ISMS). Dazu gehören die Erstellung und Wartung von Dokumentationen, Erstellung von Sicherheits- und Datensicherungskonzepten, oder auch die Durchführung laufender Protokollierungen und Monitorings. Da bereits die Etablierung eines vollständigen ISMS für Privatpersonen wenig realistisch und in den allermeisten Fällen auch nicht notwendig ist, ist dieses Kapitel für Privatpersonen kaum relevant.

13 Sicherheitsmanagement in der Kommunikation

Dieses Kapitel beschreibt einerseits Aspekte der Netzwerksicherheit und andererseits Themen im Zusammenhang mit dem sicheren elektronischen Austausch von Daten. Auch für Privatpersonen relevant ist die Sicherheit im Rahmen des elektronischen Datenaustauschs. Einzelne Elemente dieses Kapitels können daher auch für Privatpersonen interessant und hilfreich sein.

14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems

Dieses Kapitel des Sicherheitshandbuchs beschreibt relevante Aspekte bezüglich Entwicklung, Betrieb und Wartung von IT-Systemen. Während entwicklungsbezogene Aspekte primär für IT-Unternehmen von Bedeutung sind, betreffen Aspekte des Betriebs und der Wartung von IT-Systemen auch Privatpersonen, wenn auch nicht im selben Ausmaß wie Unternehmen. Dieses Kapitel kann aber auch Privatpersonen positive Impulse für eine sichere Verwendung ihrer privaten IT-Geräte geben.

15 Lieferantenbeziehungen

Dieses Kapitel widmet sich Sicherheitsaspekten im Zusammenhang mit der Interaktion mit Lieferanten. Lieferantenbeziehungen spielen für Privatpersonen nur eine sehr untergeordnete Rolle. Dementsprechend sind die Inhalte dieses Kapitels für Privatpersonen kaum von Bedeutung.

16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)

Dieses Kapitel beschreibt notwendige Prozesse zum geeigneten Umgang mit Informationssicherheitsereignissen. Prinzipiell sind auch Privatpersonen nicht vor Sicherheitsvorfällen gefeit. Eine Vorbereitung auf solche Situation ist im Allgemeinen auch für Privatpersonen sinnvoll, auch wenn diese in der Regel weniger prozessorientiert sein wird als in Unternehmen. Die Lektüre dieses Kapitels kann jedoch auch Privatpersonen nützliche Inputs zur persönlichen Vorbereitung auf Sicherheitsvorfälle im privaten Bereich liefern.

17 Disaster Recovery und Business Continuity

Dieses Kapitel des Sicherheitshandbuchs beschreibt notwendige Prozesse für ein betriebliches Kontinuitätsmanagement inklusive der definierten und zeitnahen Rückkehr in den Normalbetrieb nach unvorhergesehenen Ausfällen. Diese Themen sind zwar primär für Unternehmen von Bedeutung, allerdings können Systemausfälle, z.B. ausgelöst durch Defekte eigener Hardware, auch für Privatpersonen unangenehm sein. Die in diesem Kapitel beschriebenen Methoden können auch Privatpersonen wertvolle Inputs liefern, um sich zum Beispiel über geeignete Backup-Strategien auf solche Situationen vorzubereiten.

18 Security Compliance

Dieses Kapitel definiert notwendige Überprüfungen der Einhaltung geltender Vorgaben und das laufende Monitoring der Informationssicherheit. Da im privaten Umfeld kaum formale Informationssicherheitsmanagementsysteme zum Einsatz kommen werden und auch die formale Compliance zu anderen Vorgaben eine eher untergeordnete Rolle spielt, hat dieses Kapitel für Privatpersonen wenig Relevanz.

A.1 Sicherheitsszenarien

Dieser Anhang des Sicherheitshandbuchs widmet sich Themen der industriellen Sicherheit und des E-Governments in Österreich. Für Privatpersonen haben diese Themen nur wenig Relevanz, auch da sich die in diesem Kapitel behandelten E-Government-bezogenen Themen eher an Unternehmen als an Bürgerinnen und Bürger richten.

A.2 Sicherheitstechnologien

Dieser Anhang beschreibt ausgewählte Sicherheitstechnologien. Ein tieferes Verständnis dieser Technologien ist in der Regel nicht nötig, da deren Funktionen zumeist über einschlägige Produkte bereitgestellt werden. Der Anhang kann jedoch zum prinzipiellen Verständnis der Technologien und ihrer Vor- und Nachteile beitragen und damit auch für Privatpersonen zumindest teilweise interessant sein.

A.3 Cloud Computing

Dieser Anhang diskutiert sicherheitsrelevante Aspekte aus dem Bereich Cloud Computing. Cloud Computing spielt auch für Privatpersonen eine zunehmend wichtige Rolle. Dieser Anhang bringt damit auch für Privatpersonen einen Mehrwert.

A.4 Smartphone Sicherheit

Dieser Anhang des Sicherheitshandbuchs widmet sich dem Thema Smartphone-Sicherheit. Smartphones lösen klassische Endnutzergeräte wie PCs oder Laptops auch im privaten Umfeld zunehmend als präferierte Endnutzergeräte ab. Damit ist dieser Anhang auch für Privatpersonen relevant, auch wenn sich Teile des Anhangs eher auf einen Smartphone-Einsatz in Unternehmen beziehen.

A.5 Sicherheit in sozialen Netzen
Soziale Netze spielen vor allem auch im privaten Umfeld eine wichtige Rolle. Dieser Anhang des Sicherheitshandbuchs beschreibt sicherheitsrelevante Aspekte, die im Umgang mit sozialen Netzen beachtet werden müssen und ist somit auch für Privatpersonen relevant.

A.6 Sichere Beschaffung
Auch im Rahmen von Beschaffungsvorgängen müssen diverse Aspekte der Informationssicherheit beachtet werden. Dieser Anhang geht auf diesen Umstand näher ein und definiert hierfür ein relativ formales und prozessgetriebenes Vorgehen. Für Privatpersonen spielen dieses Thema und damit auch dieser Anhang eher eine untergeordnete Rolle, einzelne Aspekte können jedoch auch für Anschaffungen im privaten Bereich einen wertvollen Input liefern.

1.3.3.3 Zielgruppe: Ein-Personen-Unternehmen (EPU)

In diesem Abschnitt wird die Relevanz der einzelnen Kapitel des Sicherheitshandbuchs aus der Sicht von Ein-Personen-Unternehmen (EPU) bewertet. Die Bewertung erfolgt über eine dreistufige Farbskala. Grün symbolisiert, dass das betreffende Kapitel und das darin behandelte Themengebiet für EPUs besonders relevant sind. Orange zeigt an, dass das betreffende Kapitel durchaus für EPUs relevante und interessante Inhalte umfasst, jedoch potenziell nicht alle Vorgaben aus dem Kapitel für EPUs relevant sind. Rot markiert sind schließlich jene Kapitel des Sicherheitshandbuchs, die für EPUs nur eine untergeordnete Rolle spielen, der Vollständigkeit halber jedoch natürlich trotzdem berücksichtigt werden sollten.

1 Einführung
Dieses erste Kapitel des Sicherheitshandbuchs enthält allgemeine Informationen und Einführungen, die sich an alle Zielgruppen richten und damit auch für EPUs relevant sind.

2 Informationssicherheitsmanagementsystem (ISMS)
Dieses Kapitel beschreibt Konzepte eines Informationssicherheitsmanagementsystems (ISMS). Die Etablierung und der Betrieb eines vollständigen ISMS ist für EPUs wohl in den meisten Fällen zu viel des Guten. Diese Kapitel spielt für EPUs daher eher eine untergeordnete Rolle.

3 Managementverantwortung und Aufgaben beim ISMS

Dieses Kapitel beschreibt im Detail die Aufgaben des Managements im Rahmen eines ISMS. Da vollständige ISMS für EPUs wohl meist nur eine untergeordnete Rolle spielen und EPUs in der Regel auch über keine umfangreichen und verteilten Managementstrukturen verfügen, kann die Relevanz dieses Kapitels für EPUs als gering eingeschätzt werden.

4 Informationssicherheitspolitik
Dieses Kapitel widmet sich der Erstellung und laufenden Wartung einer unternehmensweiten Informationssicherheitspolitik (Security Policy). Auch wenn die formale Erstellung und Wartung eines entsprechenden Dokuments für EPUs wohl übertrieben wäre, ist die prinzipielle zugrunde liegende Idee – nämlich die Definition des eigenen Zugangs zum Thema Informationssicherheit und der damit verbundenen Erwartungshaltungen und Ziele – auch für EPUs durchaus sinnvoll.

5 Risikomanagement
Dieses Kapitel beschreibt Ansätze und Methoden der Risikoanalyse und die weitere Behandlung der identifizierten Risiken. Die Durchführung einer Risikoanalyse ist fundamental, um eigene Vermögenswerte (Assets) und deren Bedrohungen zu identifizieren und um basierend darauf geeignete Sicherheitsmaßnahmen treffen zu können. Dieses Kapitel ist damit zielgruppenunabhängig immer relevant und damit auch für EPUs von zentraler Bedeutung.

6 Organisation
Dieses Kapitel widmet sich vor allem der Frage, über welche organisatorischen Prozesse der effektive Betrieb eines ISMS in einem Unternehmen unterstützt wird. Für ein EPU ist die formale Definition solcher organisatorischen Prozesse in den meisten Fällen wohl nicht notwendig. Allerdings behandelt dieses Kapitel mit z.B. Outsourcing schon auch Themen, die sehr wohl auch für EPUs interessant und relevant sein können, auch wenn diese in einem EPU nicht notwendigerweise über formale organisatorische Prozesse abgedeckt werden müssen.

7 Personelle Sicherheit
Dieses Kapitel des Sicherheitshandbuchs widmet sich Aspekten der personellen Sicherheit, wie z.B. der Definition und Umsetzung von Regeln für Mitarbeiterinnen und Mitarbeiter. Da ein EPU per Definition über keine weiteren Mitarbeiter verfügt, ist dieser Abschnitt für EPUs wohl wenig relevant, auch wenn einzelne in diesem Abschnitt behandelte Sicherheitsaspekte – wie z.B. Clear-Desk-Policy – universelle Relevanz haben.

8 Vermögenswerte und Klassifizierung von Informationen
Dieses Kapitel widmet sich der Identifikation von Vermögenswerten (Assets) und der Bewertung ihrer Kritikalität und ihres Schutzbedarfs. Damit steht dieses Kapitel in engem Zusammenhang mit Kapitel 4 (Risikoanalyse), da die Erfassung von Vermögenswerten eine Grundvoraussetzung für die Durchführung einer Risikoanalyse ist. Wie Kapitel 4 ist auch dieses Kapitel zielgruppenunabhängig relevant und damit auch für EPUs von Bedeutung.

9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung

Dieses Kapitel adressiert die Kontrolle und Beschränkung des Zugriffs auf IT-Systeme. Dabei handelt es sich um eine für die Informationssicherheit zentrale Sicherheitsfunktion. Die Relevanz gilt unabhängig von der Organisationsgröße, auch wenn mit steigender Größe und damit zumeist einhergehender Zunahme der Komplexität der IT-Infrastruktur auch die Umsetzung einer geeigneten Zugriffskontrolle komplexer wird. Die grundlegenden Konzepte sind jedoch auch bereits für EPUs hoch relevant.

10 Kryptographie

Dieses Kapitel widmet sich dem Einsatz kryptographischer Methoden und den in diesem Zusammenhang zu beachtenden Aspekten. Kryptographische Methoden und die darauf aufbauenden Lösungen und Produkte sind das Fundament der Informationssicherheit. Die Kenntnis ihrer Möglichkeiten und Limitierungen ist daher unabhängig von der Organisationsgröße und damit im Speziellen auch für EPUs relevant.

11 Physische und umgebungsbezogene Sicherheit

Dieses Kapitel adressiert Themen der physischen und umgebungsbezogenen Sicherheit und geht im Speziellen auf Aspekte der Raum- und Gebäudesicherheit ein. Diese Themen sind speziell relevant für größere Unternehmen, die über umfangreiche Betriebsstätten (Bürogebäude, Serverräume, Rechenzentren, etc.) verfügen. Für EPUs ist die Relevanz damit nur bedingt gegeben, einzelne Aspekte der Raum- und Gebäudesicherheit können jedoch auch für EPUs schon von Bedeutung sein.

12 Sicherheitsmanagement im Betrieb

Dieses Kapitel des Sicherheitshandbuchs widmet sich relevanten Aspekten des Betriebs eines Informationssicherheitsmanagementsystems (ISMS). Dazu gehören die Erstellung und Wartung von Dokumentationen, Erstellung von Sicherheits- und Datensicherungskonzepten, oder auch die Durchführung laufender Protokollierungen und Monitorings. Da bereits die Etablierung eines vollständigen ISMS für EPUs als zumeist nicht notwendig festgestellt wurde, sprengen auch die in diesem Kapitel beschriebenen Tätigkeiten in der Regel die Grenzen und Möglichkeiten eines EPU. Trotzdem sind einzelne in diesem Kapitel beschriebene Tätigkeiten auch für EPUs sinnvoll, auch wenn diese nicht vollumfänglich und im Rahmen eines vollständigen ISMS umgesetzt werden müssen.

13 Sicherheitsmanagement in der Kommunikation

Dieses Kapitel beschreibt einerseits Aspekte der Netzwerksicherheit und andererseits Themen im Zusammenhang mit dem sicheren elektronischen Austausch von Daten. Während Netzwerksicherheit auch für EPUs grundsätzlich relevant ist, ergeben sich für diese wohl in der Regel weniger konkrete Anforderungen als für größere Unternehmen mit komplexen Netzwerkinfrastrukturen. Trotzdem sollten auch für EPUs Konzepte der Netzwerksicherheit bekannt sein. In jedem Fall hoch relevant und das unabhängig von der Unternehmensgröße ist die Sicherheit im Rahmen des elektronischen Datenaustauschs. Insgesamt kann dieses Kapitel auch für EPUs damit als wichtig angesehen werden.

14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems

Dieses Kapitel des Sicherheitshandbuchs beschreibt relevante Aspekte bezüglich Entwicklung, Betrieb und Wartung von IT-Systemen. Während entwicklungsbezogene Aspekte primär für IT-Unternehmen von Bedeutung sind, betreffen Aspekte des Betriebs und der Wartung von IT-Systemen Unternehmen nahezu aller Branchen. Dies auch unabhängig von ihrer Größe. Dementsprechend kann dieses Kapitel auch für EPUs als relevant angesehen werden.

15 Lieferantenbeziehungen

Dieses Kapitel widmet sich Sicherheitsaspekten im Zusammenhang mit der Interaktion mit Lieferanten. Schnittstellen zu Lieferanten können sich für alle Unternehmen unabhängig von ihrer Größe ergeben. Dementsprechend sind die Inhalte dieses Kapitels auch für EPUs von Bedeutung.

16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)

Dieses Kapitel beschreibt notwendige Prozesse zum geeigneten Umgang mit Informationssicherheitsereignissen. Prinzipiell ist dieses Thema auch für EPUs relevant, da diese vor solchen Vorfällen nicht gefeit sind. Allerdings ist für EPUs wohl in der Regel ein weniger prozessgetriebener Ansatz zum Umgang mit solchen Vorfällen sinnvoll. In jedem Fall sollten jedoch auch EPUs auf unvorhergesehene Ereignisse entsprechend vorbereitet sein. Die in diesem Kapitel beschriebenen Ansätze können hierfür auch für EPUs ein wertvoller Input sein.

17 Disaster Recovery und Business Continuity

Dieses Kapitel des Sicherheitshandbuchs beschreibt notwendige Prozesse für ein betriebliches Kontinuitätsmanagement inklusive der definierten und zeitnahen Rückkehr in den Normalbetrieb nach unvorhergesehenen Ausfällen. Diese Themen sind prinzipiell auch für EPUs relevant, allerdings ist für diese aufgrund der in der Regel weniger komplexen IT-Infrastruktur meist ein einfacherer und weniger prozessgetriebener Ansatz ausreichend. Die in diesem Kapitel beschriebenen Methoden können jedoch auch für EPUs ein wertvoller Input sein.

18 Security Compliance

Dieses Kapitel definiert notwendige Überprüfungen der Einhaltung geltender Vorgaben und das laufende Monitoring der Informationssicherheit. Da in EPUs in der Regel ein weniger formaler und weniger prozessgetriebener Ansatz verfolgt werden kann, spielen in diesen Unternehmen formale Compliance-Checks und systematische Monitorings nur eine untergeordnete Rolle. Dies auch deshalb, weil in EPUs nur in den seltensten Fällen ein vollständiges ISMS zum Einsatz kommen wird.

A.1 Sicherheitsszenarien

Dieser Anhang des Sicherheitshandbuchs widmet sich Themen der industriellen Sicherheit und des E-Governments in Österreich. Für EPUs haben diese Themen nur wenig Relevanz.

A.2 Sicherheitstechnologien

Dieser Anhang beschreibt ausgewählte Sicherheitstechnologien. Ein tieferes Verständnis dieser Technologien ist in der Regel nicht nötig, da deren Funktionen zumeist über einschlägige Produkte bereitgestellt werden. Der Anhang kann jedoch zum prinzipiellen Verständnis der Technologien und ihrer Vor- und Nachteile beitragen.

A.3 Cloud Computing
Dieser Anhang diskutiert sicherheitsrelevante Aspekte aus dem Bereich Cloud Computing. Cloud Computing spielt für alle Unternehmen unabhängig von ihrer Größe eine zunehmend wichtige Rolle. Dieser Anhang richtet sich damit implizit auch an EPUs.

A.4 Smartphone Sicherheit
Dieser Anhang des Sicherheitshandbuchs widmet sich dem Thema Smartphone-Sicherheit. Smartphones lösen klassische Endnutzergeräte wie PCs oder Laptops zunehmend als präferierte Endnutzergeräte ab und spielen auch in Unternehmen unabhängig von ihrer Größe eine immer wichtigere Rolle. Damit ist dieser Anhang auch für EPUs hoch relevant.

A.5 Sicherheit in sozialen Netzen
Soziale Netze spielen auch im beruflichen Umfeld und für Unternehmen eine zunehmend wichtige Rolle. Dieser Anhang des Sicherheitshandbuchs beschreibt sicherheitsrelevante Aspekte, die dabei beachtet werden müssen. Diese sind unabhängig von der Größe des Unternehmens und damit auch für EPUs von Bedeutung.

A.6 Sichere Beschaffung
Auch im Rahmen von Beschaffungsvorgängen müssen diverse Aspekte der Informationssicherheit beachtet werden. Dieser Anhang geht auf diesen Umstand näher ein und definiert hierfür ein relativ formales und prozessgetriebenes Vorgehen. Auch für EPUs sind diese Themen relevant, allerdings sind für diese in der Regel weniger formale Ansätze realistischer. Der Anhang kann jedoch auch für EPUs wertvolle Inputs für die Etablierung von Beschaffungsprozessen liefern, auch wenn diese in der Praxis bei EPUs potenziell weniger formal umgesetzt werden.

1.3.3.4 Zielgruppe: Kleine und mittlere Unternehmen (KMU)

In diesem Abschnitt wird die Relevanz der einzelnen Kapitel des Sicherheitshandbuchs aus der Sicht von kleinen und mittleren Unternehmen (KMU) bewertet. Die Bewertung erfolgt wiederum über eine dreistufige Farbskala. Grün symbolisiert, dass das betreffende Kapitel und das darin behandelte Themengebiet für KMUs besonders relevant sind. Orange zeigt an, dass das betreffende Kapitel zwar für KMUs relevante und interessante Inhalte umfasst, jedoch potenziell nicht alle Vorgaben aus dem Kapitel für KMUs relevant sind. Rot markiert sind schließlich jene Kapitel des Sicherheitshandbuchs, die für KMUs nur eine untergeordnete Rolle spielen, der Vollständigkeit halber jedoch natürlich trotzdem berücksichtigt werden sollten.

1 Einführung
Dieses erste Kapitel des Sicherheitshandbuchs enthält allgemeine Informationen und Einführungen, die sich an alle Zielgruppen richten. Damit ist es auch für KMUs relevant.

2 Informationssicherheitsmanagementsystem (ISMS)

Dieses Kapitel beschreibt Konzepte eines Informationssicherheitsmanagementsystems (ISMS). Die Etablierung und der Betrieb eines vollständigen ISMS kann abhängig von der Unternehmensgröße die Möglichkeiten von KMUs übersteigen. Trotzdem sollten auch bereits KMUs ihren Umgang mit dem Thema Informationssicherheit so systematisch und methodisch wie möglich anlegen. Ein ISMS kann dabei einen geeigneten Rahmen vorgeben, auch wenn dieses nicht vollständig umgesetzt wird. Die Informationen dieses Kapitels können KMUs daher nützliche Informationen liefern.

3 Managementverantwortung und Aufgaben beim ISMS

Dieses Kapitel beschreibt im Detail die Aufgaben des Managements im Rahmen eines ISMS. Die in diesem Kapitel beschriebenen Aufgaben innerhalb eines ISMS sind auch für KMUs relevant. Je nach Größe des Unternehmens und seiner Management-Struktur können die Vorgaben aus diesem Kapitel des Sicherheitshandbuchs jedoch punktuell die Möglichkeiten des Unternehmens übersteigen. In jedem Fall enthält das Kapitel für KMUs relevante Informationen, auch wenn nicht alle Vorgaben daraus dann tatsächlich umgesetzt werden.

4 Informationssicherheitspolitik

Dieses Kapitel widmet sich der Erstellung und laufenden Wartung einer unternehmensweiten Informationssicherheitspolitik (Security Policy). Auch wenn die formale Erstellung und Wartung eines entsprechenden Dokuments KMUs je nach deren Größe und Organisationsstruktur noch überfordern kann, ist die prinzipielle zugrunde liegende Idee – nämlich die Definition des eigenen Zugangs zum Thema Informationssicherheit und der damit verbundenen Erwartungshaltungen und Ziele – in jedem Fall auch für KMUs sinnvoll.

5 Risikomanagement

Dieses Kapitel beschreibt Ansätze und Methoden der Risikoanalyse und die weitere Behandlung der identifizierten Risiken. Die Durchführung einer Risikoanalyse ist fundamental, um eigene Vermögenswerte (Assets) und deren Bedrohungen zu identifizieren und um basierend darauf geeignete Sicherheitsmaßnahmen treffen zu können. Dieses Kapitel ist damit zielgruppenunabhängig immer relevant und damit auch für KMUs von zentraler Bedeutung.

6 Organisation

Dieses Kapitel widmet sich vor allem der Frage, über welche organisatorischen Prozesse der effektive Betrieb eines ISMS in einem Unternehmen unterstützt wird. Für ein KMU kann die formale Definition solcher organisatorischen Prozesse je nach Unternehmensgröße noch nicht notwendig sein. Dieses Kapitel behandelt jedoch mit z.B. Outsourcing auch Themen, die sehr wahrscheinlich für KMUs interessant und relevant sein können, selbst wenn diese aufgrund der geringen Unternehmensgröße noch nicht notwendigerweise über formale organisatorische Prozesse abgedeckt werden müssen.

7 Personelle Sicherheit

Dieses Kapitel des Sicherheitshandbuchs widmet sich Aspekten der personellen Sicherheit, wie z.B. der Definition und Umsetzung von Regeln für Mitarbeiterinnen und Mitarbeiter. Da KMUs in der Regel über Mitarbeiter verfügen, ist dieser Themenbereich für KMUs auch relevant. Je nach Unternehmensgröße kann dabei ein mehr oder weniger formaler Zugang zu diesem Thema sinnvoll sein. Die in diesem Kapitel adressierten Aspekte sind jedoch in jedem Fall beachtenswert.

8 Vermögenswerte und Klassifizierung von Informationen

Dieses Kapitel widmet sich der Identifikation von Vermögenswerten (Assets) und der Bewertung ihrer Kritikalität und ihres Schutzbedarfs. Damit steht dieses Kapitel in engem Zusammenhang mit Kapitel 4 (Risikoanalyse), da die Erfassung von Vermögenswerten eine Grundvoraussetzung für die Durchführung einer Risikoanalyse ist. Wie Kapitel 4 ist auch dieses Kapitel zielgruppenunabhängig relevant und damit auch für KMUs von Bedeutung.

9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung

Dieses Kapitel adressiert die Kontrolle und Beschränkung des Zugriffs auf IT-Systeme. Dabei handelt es sich um eine für die Informationssicherheit zentrale Sicherheitsfunktion. Die Relevanz gilt unabhängig von der Organisationsgröße, auch wenn mit steigender Größe und damit zumeist einhergehender Zunahme der Komplexität der IT-Infrastruktur auch die Umsetzung einer geeigneten Zugriffskontrolle komplexer wird. Die grundlegenden Konzepte sind jedoch in jedem Fall für KMUs hoch relevant.

10 Kryptographie

Dieses Kapitel widmet sich dem Einsatz kryptographischer Methoden und den in diesem Zusammenhang zu beachtenden Aspekten. Kryptographische Methoden und die darauf aufbauenden Lösungen und Produkte sind das Fundament der Informationssicherheit. Die Kenntnis ihrer Möglichkeiten und Limitierungen ist daher unabhängig von der Organisationsgröße und damit im Speziellen auch für KMUs sinnvoll.

11 Physische und umgebungsbezogene Sicherheit

Dieses Kapitel adressiert Themen der physischen und umgebungsbezogenen Sicherheit und geht im Speziellen auf Aspekte der Raum- und Gebäudesicherheit ein. Diese Themen sind speziell relevant für größere Unternehmen, die über umfangreiche Betriebsstätten (Bürogebäude, Serverräume, Rechenzentren, etc.) verfügen. Auch KMUs verfügen jedoch der Regel über eine wenn auch kleinere Gebäudeinfrastruktur, deren Sicherheit eine direkte Auswirkung auf die Informationssicherheit haben kann. Dieses Kapitel ist damit auch für KMUs von Bedeutung.

12 Sicherheitsmanagement im Betrieb

Dieses Kapitel des Sicherheitshandbuchs widmet sich relevanten Aspekten des Betriebs eines Informationssicherheitsmanagementsystems (ISMS). Dazu gehören die Erstellung und Wartung von Dokumentationen, Erstellung von Sicherheits- und Datensicherungskonzepten, oder auch die Durchführung laufender Protokollierungen und Monitorings. Da die Etablierung eines vollständigen ISMS für KMUs abhängig von ihrer Größe nicht immer möglich ist, können auch die in diesem

Kapitel beschriebenen Tätigkeiten potenziell die Möglichkeiten eines KMU übersteigen. Trotzdem sind einzelne in diesem Kapitel beschriebene Tätigkeiten in jedem Fall auch für KMUs sinnvoll, selbst wenn diese nicht vollumfänglich und im Rahmen eines vollständigen ISMS umgesetzt werden.

13 Sicherheitsmanagement in der Kommunikation

Dieses Kapitel beschreibt einerseits Aspekte der Netzwerksicherheit und andererseits Themen im Zusammenhang mit dem sicheren elektronischen Austausch von Daten. Während Netzwerksicherheit auch für KMUs grundsätzlich relevant ist, ergeben sich für diese oft noch weniger konkrete Anforderungen als für große Unternehmen mit komplexen Netzwerkinfrastrukturen. Trotzdem sollten auch für KMUs Konzepte der Netzwerksicherheit bekannt sein und zur Umsetzung kommen. In jedem Fall hoch relevant, und das unabhängig von der Unternehmensgröße, ist die Sicherheit im Rahmen des elektronischen Datenaustauschs. Insgesamt ergibt sich für dieses Kapitel damit eine hohe Relevanz für KMUs.

14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems

Dieses Kapitel des Sicherheitshandbuchs beschreibt relevante Aspekte bezüglich Entwicklung, Betrieb und Wartung von IT-Systemen. Während entwicklungsbezogene Aspekte primär für IT-Unternehmen von Bedeutung sind, betreffen Aspekte des Betriebs und der Wartung von IT-Systemen Unternehmen nahezu aller Branchen - dies auch unabhängig von ihrer Größe. Dementsprechend kann dieses Kapitel auch für KMUs als relevant angesehen werden.

15 Lieferantenbeziehungen

Dieses Kapitel widmet sich Sicherheitsaspekten betreffend die Interaktion mit Lieferanten. Schnittstellen zu Lieferanten können sich für alle Unternehmen unabhängig von ihrer Größe ergeben. Dementsprechend sind die Inhalte dieses Kapitels auch für KMUs von Bedeutung.

16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)

Dieses Kapitel beschreibt notwendige Prozesse zum geeigneten Umgang mit Informationssicherheitsereignissen. Prinzipiell ist dieses Thema auch für KMUs relevant, da diese vor solchen Vorfällen nicht gefeit sind. Allerdings kann für KMUs je nach Unternehmensgröße ein weniger prozessgetriebener Ansatz zum Umgang mit solchen Vorfällen noch sinnvoll und praktisch umsetzbar sein. In jedem Fall sollten KMUs auf unvorhergesehene Ereignisse entsprechend vorbereitet sein. Die in diesem Kapitel beschriebenen Ansätze können hierfür ein wertvoller Input sein, selbst wenn nicht alle Prozesse exakt wie im Kapitel beschrieben umgesetzt werden können.

17 Disaster Recovery und Business Continuity

Dieses Kapitel des Sicherheitshandbuchs beschreibt notwendige Prozesse für ein betriebliches Kontinuitätsmanagement inklusive der definierten und zeitnahen Rückkehr in den Normalbetrieb nach unvorhergesehenen Ausfällen. Diese Themen sind prinzipiell auch für KMUs relevant, allerdings kann für diese bei kleineren Unternehmensgrößen und weniger komplexen IT-Infrastrukturen auch ein einfacherer und weniger prozessgetriebener Ansatz ausreichend sein. Die in diesem Kapitel beschriebenen Methoden können aber in jedem Fall ein wertvoller Input sein.

18 Security Compliance

Dieses Kapitel definiert notwendige Überprüfungen der Einhaltung geltender Vorgaben und das laufende Monitoring der Informationssicherheit. Je nach Größe kann in KMUs auch ein weniger formaler und weniger prozessgetriebener Ansatz verfolgt werden. In diesem Fall spielen formale Compliance-Checks und systematische Monitorings eine weniger wichtige Rolle. Dies vor allem dann, wenn in KMUs kein vollständiges ISMS zum Einsatz kommt.

A.1 Sicherheitsszenarien

Dieser Anhang des Sicherheitshandbuchs widmet sich Themen der industriellen Sicherheit und des E-Governments in Österreich. Für KMUs dürften diese Themen in der Regel nur wenig Relevanz haben, außer diese sind in diesen konkreten Bereichen tätig.

A.2 Sicherheitstechnologien

Dieser Anhang beschreibt ausgewählte Sicherheitstechnologien. Ein tieferes Verständnis dieser Technologien ist in der Regel nicht nötig, da deren Funktionen zumeist über einschlägige Produkte bereitgestellt werden. Der Anhang kann jedoch zum prinzipiellen Verständnis der Technologien und ihrer Vor- und Nachteile beitragen.

A.3 Cloud Computing

Dieser Anhang diskutiert sicherheitsrelevante Aspekte aus dem Bereich Cloud Computing. Cloud Computing spielt für alle Unternehmen unabhängig von ihrer Größe eine zunehmend wichtige Rolle. Dieser Anhang ist damit insbesondere auch für KMUs von Bedeutung.

A.4 Smartphone Sicherheit

Dieser Anhang des Sicherheitshandbuchs widmet sich dem Thema Smartphone-Sicherheit. Smartphones lösen klassische Endnutzergeräte wie PCs oder Laptops zunehmend als präferierte Endnutzergeräte ab und spielen auch in Unternehmen unabhängig von ihrer Größe eine immer wichtigere Rolle. Damit ist dieser Anhang auch für KMUs hoch relevant.

A.5 Sicherheit in sozialen Netzen

Soziale Netze spielen auch im beruflichen Umfeld und für Unternehmen eine zunehmend wichtige Rolle. Dieser Anhang des Sicherheitshandbuchs beschreibt sicherheitsrelevante Aspekte, die dabei beachtet werden müssen. Diese sind unabhängig von der Größe des Unternehmens und damit auch für KMUs von Bedeutung.

A.6 Sichere Beschaffung

Auch im Rahmen von Beschaffungsvorgängen müssen diverse Aspekte der Informationssicherheit beachtet werden. Dieser Anhang geht auf diesen Umstand näher ein und definiert hierfür ein relativ formales und prozessgetriebenes Vorgehen. Auch für KMUs sind diese Themen relevant, allerdings sind für diese oft auch noch weniger formale Ansätze geeignet. Der Anhang kann jedoch für KMUs jedenfalls wertvolle Inputs für die Etablierung von Beschaffungsprozessen liefern, selbst wenn diese etwa aufgrund einer geringen Unternehmensgröße weniger formal umgesetzt werden.

1.3.3.5 Zielgruppe: Großunternehmen und Behörden

In diesem Abschnitt wird die Relevanz der einzelnen Kapitel des Sicherheitshandbuchs aus der Sicht von Großunternehmen bzw. Behörden mit einer großen Anzahl an Mitarbeiterinnen und Mitarbeitern, einem breiten Betätigungsfeld, sowie komplexer Organisations- und Managementstrukturen bewertet. Die Bewertung erfolgt wiederum über eine dreistufige Farbskala. Grün symbolisiert, dass das betreffende Kapitel und das darin behandelte Themengebiet für Großunternehmen und Behörden besonders relevant sind. Orange zeigt an, dass das betreffende Kapitel zwar für Großunternehmen und Behörden relevante und interessante Inhalte umfasst, jedoch potenziell nicht alle Vorgaben aus dem Kapitel von Bedeutung sind. Rot markiert sind schließlich jene Kapitel des Sicherheitshandbuchs, die für Großunternehmen oder Behörden nur eine untergeordnete Rolle spielen, der Vollständigkeit halber jedoch natürlich trotzdem berücksichtigt werden sollten.

Aus untenstehender Tabelle wird ersichtlich, dass für Großunternehmen und Behörden prinzipiell alle Kapitel und Themen des Sicherheitshandbuchs von Bedeutung sind. Natürlich können sich im Einzelfall auch für Großunternehmen oder Behörden je nach ihrem Tätigkeitsbereich und ihrer Organisation einzelne Aspekte mit geringerer Relevanz ergeben. Insgesamt ist es ab einer gewissen Unternehmens- bzw. Organisationsgröße aber in jedem Fall sinnvoll, sämtliche Inhalte des Sicherheitshandbuchs explizit auf ihre Relevanz in Bezug auf das Unternehmen bzw. die Organisation zu prüfen.

Auch wenn für Großunternehmen und Behörden im Allgemeinen alle Kapitel und Themen des Sicherheitshandbuchs als relevant angesehen werden können, wird auf die einzelnen Kapitel in untenstehender Tabelle trotzdem nochmal explizit eingegangen, um deren Relevanz speziell im Kontext von Großunternehmen und Behörden herauszuarbeiten.

1 Einführung
Dieses erste Kapitel des Sicherheitshandbuchs enthält allgemeine Informationen und Einführungen, die sich an alle Zielgruppen richten. Damit ist es auch für Großunternehmen und Behörden relevant.

2 Informationssicherheitsmanagementsystem (ISMS)
Dieses Kapitel beschreibt Konzepte eines Informationssicherheitsmanagementsystems (ISMS). Die Etablierung und der Betrieb eines vollständigen ISMS ist ein komplexes und aufwändiges Unterfangen, ab einer gewissen Unternehmensgröße jedoch in jedem Fall ratsam. Über ein ISMS kann ein systematischer und methodischer Umgang mit dem Thema Informationssicherheit sichergestellt werden. Ein solcher ist speziell für Großunternehmen und Behörden aufgrund ihrer Größe und Komplexität essenziell. Die Informationen dieses Kapitels können daher nützliche Informationen im Zusammenhang mit der Etablierung eines ISMS liefern.

3 Managementverantwortung und Aufgaben beim ISMS
Dieses Kapitel beschreibt im Detail die Aufgaben des Managements im Rahmen eines ISMS. Die in diesem Kapitel beschriebenen Aufgaben innerhalb eines ISMS sind damit speziell auch für Großunternehmen und Behörden relevant, die in der Regel über komplexe Managementstrukturen und wohldefinierte Managementprozesse verfügen.

4 Informationssicherheitspolitik
Dieses Kapitel widmet sich der Erstellung und laufenden Wartung einer unternehmensweiten Informationssicherheitspolitik (Security Policy). Die Definition und interne Kommunikation des eigenen Zugangs zum Thema Informationssicherheit und der damit verbundenen Erwartungshaltungen und Ziele, ist für alle Unternehmen sinnvoll. Bei Großunternehmen und Behörden empfiehlt sich dafür im Speziellen die Erstellung einer expliziten Informationssicherheitspolitik (Security Policy) entsprechend der Beschreibung in diesem Kapitel des Sicherheitshandbuchs.

5 Risikomanagement
Dieses Kapitel beschreibt Ansätze und Methoden der Risikoanalyse und die weitere Behandlung der identifizierten Risiken. Die Durchführung einer Risikoanalyse ist fundamental, um eigene Vermögenswerte (Assets) und deren Bedrohungen zu identifizieren und um basierend darauf geeignete Sicherheitsmaßnahmen treffen zu können. Dieses Kapitel ist damit zielgruppenunabhängig immer relevant. Speziell gilt dies auch für Großunternehmen und Behörden, die in der Regel über eine Vielzahl an Vermögenswerten verfügen.

6 Organisation
Dieses Kapitel widmet sich vor allem der Frage, über welche organisatorischen Prozesse der effektive Betrieb eines ISMS in einem Unternehmen unterstützt wird. Ab einer gewissen Unternehmensgröße ist die formale Definition solcher organisatorischen Prozesse in jedem Fall sinnvoll. Dieses Kapitel kann dabei unterstützen.

7 Personelle Sicherheit
Dieses Kapitel des Sicherheitshandbuchs widmet sich Aspekten der personellen Sicherheit, wie z.B. der Definition und Umsetzung von Regeln für Mitarbeiterinnen und Mitarbeiter. Da sowohl Großunternehmen als auch Behörden in der Regel über eine große Anzahl an Mitarbeiterinnen und Mitarbeitern verfügen, ist dieser Themenbereich für diese Organisationen speziell relevant.

8 Vermögenswerte und Klassifizierung von Informationen
Dieses Kapitel widmet sich der Identifikation von Vermögenswerten (Assets) und der Bewertung ihrer Kritikalität und ihres Schutzbedarfs. Damit steht dieses Kapitel in engem Zusammenhang mit Kapitel 4 (Risikoanalyse), da die Erfassung von Vermögenswerten eine Grundvoraussetzung für die Durchführung einer Risikoanalyse ist. Wie Kapitel 4 ist auch dieses Kapitel zielgruppenunabhängig relevant und damit im Speziellen auch für Großunternehmen und Behörden von Bedeutung.

9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung
Dieses Kapitel adressiert die Kontrolle und Beschränkung des Zugriffs auf IT-Systeme. Dabei handelt es sich um eine für die Informationssicherheit zentrale Sicherheitsfunktion. Die Relevanz gilt unabhängig von der Organisationsgröße, auch wenn mit steigender Größe und damit zumeist einhergehender Zunahme der Komplexität der IT-Infrastruktur auch die Umsetzung einer geeigneten Zugriffskontrolle komplexer wird. Damit sind dieser Themenbereich und das entsprechende Kapitel des Sicherheitshandbuchs speziell für Großunternehmen und Behörden hoch relevant.

10 Kryptographie
Dieses Kapitel widmet sich dem Einsatz kryptographischer Methoden und den in diesem Zusammenhang zu beachtenden Aspekten. Kryptographische Methoden und die darauf aufbauenden Lösungen und Produkte sind das Fundament der Informationssicherheit. Die Kenntnis ihrer Möglichkeiten und Limitierungen ist daher unabhängig von der Organisationsgröße und damit im Speziellen auch für Großunternehmen und Behörden sinnvoll.

11 Physische und umgebungsbezogene Sicherheit
Dieses Kapitel adressiert Themen der physischen und umgebungsbezogenen Sicherheit und geht im Speziellen auf Aspekte der Raum- und Gebäudesicherheit ein. Diese Themen und das entsprechende Kapitel des Sicherheitshandbuchs sind insbesondere relevant für Großunternehmen, die über umfangreiche Betriebsstätten (Bürogebäude, Serverräume, Rechenzentren, etc.) verfügen.

12 Sicherheitsmanagement im Betrieb
Dieses Kapitel des Sicherheitshandbuchs widmet sich relevanten Aspekten des Betriebs eines Informationssicherheitsmanagementsystems (ISMS). Dazu gehören die Erstellung und Wartung von Dokumentationen, Erstellung von Sicherheits- und Datensicherungskonzepten, oder auch die Durchführung laufender Protokollierungen und Monitorings. Da die Etablierung eines vollständigen ISMS für Unternehmen ab einer gewissen Größe in jedem Fall ratsam ist, sind die in diesem Kapitel beschriebenen Tätigkeiten in jedem Fall für Großunternehmen und Behörden relevant.

13 Sicherheitsmanagement in der Kommunikation
Dieses Kapitel beschreibt einerseits Aspekte der Netzwerksicherheit und andererseits Themen im Zusammenhang mit dem sicheren elektronischen Austausch von Daten. Beide Themenbereiche sind für Großunternehmen und Behörden hoch relevant. Einerseits verfügen diese in der Regel über komplexe Netzwerkinfrastrukturen, andererseits sind auch Aspekte der Sicherheit des elektronischen Datenaustauschs von zentraler Bedeutung. Insgesamt ergibt sich für dieses Kapitel damit eine hohe Relevanz für Großunternehmen und Behörden.

14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems
Dieses Kapitel des Sicherheitshandbuchs beschreibt relevante Aspekte bezüglich Entwicklung, Betrieb und Wartung von IT-Systemen. Während entwicklungsbezogene Aspekte primär für IT-Unternehmen von Bedeutung sind, betreffen Aspekte des Betriebs und der Wartung von IT-Systemen Unternehmen nahezu aller Branchen. Dies auch unabhängig von ihrer Größe, wobei in Großunternehmen IT-Systeme in der Regel in größerem Umfang betrieben werden. Dementsprechend ist dieses Kapitel für Großunternehmen speziell relevant.

15 Lieferantenbeziehungen
Dieses Kapitel widmet sich Sicherheitsaspekten im Zusammenhang mit der Interaktion mit Lieferanten. Schnittstellen zu Lieferanten können sich für alle Unternehmen unabhängig von ihrer Größe ergeben. Im Speziellen sind die Inhalte dieses Kapitels auch für Großunternehmen und Behörden von Bedeutung.

16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)
Dieses Kapitel beschreibt notwendige Prozesse zum geeigneten Umgang mit Informationssicherheitsereignissen. Gerade für Großunternehmen und Behörden mit komplexer Organisationsstruktur und IT-Infrastruktur ist ein prozessgetriebener Ansatz zum Umgang mit solchen Vorfällen sinnvoll. Die in diesem Kapitel beschriebenen Ansätze können für die Etablierung entsprechender Prozesse im Unternehmen bzw. der Organisation ein wertvoller Input sein.

17 Disaster Recovery und Business Continuity
Dieses Kapitel des Sicherheitshandbuchs beschreibt notwendige Prozesse für ein betriebliches Kontinuitätsmanagement inklusive der definierten und zeitnahen Rückkehr in den Normalbetrieb nach unvorhergesehenen Ausfällen. Diese Themen sind speziell für Großunternehmen oder Behörden mit komplexer IT-Infrastruktur relevant, da in der Regel diverse Geschäftsprozesse von einer funktionierenden IT-Infrastruktur abhängen. Die in diesem Kapitel beschriebenen Methoden können ein wertvoller Input für die Etablierung entsprechender Prozesse sein.

18 Security Compliance
Dieses Kapitel definiert notwendige Überprüfungen der Einhaltung geltender Vorgaben und das laufende Monitoring der Informationssicherheit. Da für Großunternehmen und Behörden die Etablierung eines vollständigen ISMS in der Regel sinnvoll ist, sind auch die in diesem Kapitel beschriebenen Methoden zur Sicherstellung der notwendigen Compliance für Großunternehmen und Behörden relevant.

A.1 Sicherheitsszenarien
Dieser Anhang des Sicherheitshandbuchs widmet sich Themen der industriellen Sicherheit und des E-Governments in Österreich. Für Großunternehmen dürften in der Regel zumindest Aspekte der industriellen Sicherheit von Bedeutung sein, für Behörden wiederum die Schnittstellen und Sicherheitsfunktionen für E-Government.

A.2 Sicherheitstechnologien
Dieser Anhang beschreibt ausgewählte Sicherheitstechnologien. Ein tieferes Verständnis dieser Technologien ist in der Regel nicht nötig, da deren Funktionen zumeist über einschlägige Produkte bereitgestellt werden. Der Anhang kann jedoch zum prinzipiellen Verständnis der Technologien und ihrer Vor- und Nachteile beitragen, was wiederum bei der Wahl geeigneter Produkte unterstützen kann.

A.3 Cloud Computing

Dieser Anhang diskutiert sicherheitsrelevante Aspekte aus dem Bereich Cloud Computing. Cloud Computing spielt für alle Unternehmen unabhängig von ihrer Größe eine zunehmend wichtige Rolle. Dieser Anhang richtet sich damit implizit auch an Großunternehmen.

A.4 Smartphone Sicherheit

Dieser Anhang des Sicherheitshandbuchs widmet sich dem Thema Smartphone-Sicherheit. Smartphones lösen klassische Endnutzergeräte wie PCs oder Laptops zunehmend als präferierte Endnutzergeräte ab und spielen auch in Unternehmen bzw. Organisationen unabhängig von ihrer Größe eine immer wichtigere Rolle. Damit ist dieser Anhang sowohl für Großunternehmen als auch Behörden hoch relevant.

A.5 Sicherheit in sozialen Netzen

Soziale Netze spielen auch im beruflichen Umfeld, für Behörden und für Unternehmen eine zunehmend wichtige Rolle. Dieser Anhang des Sicherheitshandbuchs beschreibt sicherheitsrelevante Aspekte, die dabei beachtet werden müssen. Diese sind unabhängig von der Größe der Organisation und damit auch für Großunternehmen und Behörden von Bedeutung.

A.6 Sichere Beschaffung

Auch im Rahmen von Beschaffungsvorgängen müssen diverse Aspekte der Informationssicherheit beachtet werden. Dieser Anhang geht auf diesen Umstand näher ein und definiert hierfür ein relativ formales und prozessgetriebenes Vorgehen. Der Anhang kann damit für Großunternehmen und Behörden, die in der Regel über wohldefinierte Beschaffungsprozesse verfügen, wertvolle Inputs für die Absicherung dieser Prozesse liefern.

2 Informationssicherheitsmanagementsystem (ISMS)

2.1 Der Informationssicherheitsmanagementprozess

Informationen und die sie verarbeitenden Prozesse, Systeme und Netzwerke sind wichtige Werte jeder Organisation, sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft. Informationssicherheitsmanagement (ISM) soll die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und der sie verarbeitenden Systeme gewährleisten. Fallweise können auch weitere Anforderungen wie Zurechenbarkeit, Authentizität und Zuverlässigkeit bestehen.

Informationssicherheitsmanagement ist ein kontinuierlicher Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Zentrale Aktivitäten im Rahmen des ISMS sind:

- die Entwicklung einer organisationsweiten Informationssicherheitspolitik
- die Durchführung einer Risikoanalyse
- die Erstellung eines Sicherheitskonzeptes
- die Umsetzung der Sicherheitsmaßnahmen
- die Gewährleistung der Informationssicherheit im laufenden Betrieb
- die kontinuierliche Überwachung und Verbesserung des ISMS

Der nachfolgend dargestellte Prozess basiert auf internationalen Standards und Leitlinien zum Informationssicherheitsmanagement, insbesondere den [ISO/IEC 27001], sowie auch noch den „Guidelines on the Management of IT Security (GMITS)“ ([ISO/IEC 13335]). Er kann sowohl auf eine gesamte Organisation als auch auf Teilbereiche Anwendung finden.

Über die Anwendung auf Ebene einzelner Behörden, Abteilungen oder anderer Organisationseinheiten ist dann im spezifischen Zusammenhang - abhängig vom IT-Konzept und den bestehenden Sicherheitsanforderungen - zu entscheiden.

Das nachfolgende Bild zeigt die wichtigsten Aktivitäten im Rahmen des Informationssicherheitsmanagements und die eventuell erforderlichen Rückkopplungen zwischen den einzelnen Stufen.

Im Folgenden wird, wenn nicht ausdrücklich anders angeführt, allgemein der Begriff „Organisation“ (oder synonym dazu „Institution“) verwendet, wobei aber zu beachten ist, dass damit unterschiedliche Organisationseinheiten (Behörden, Unternehmen, Abteilungen, …) gemeint sein können.

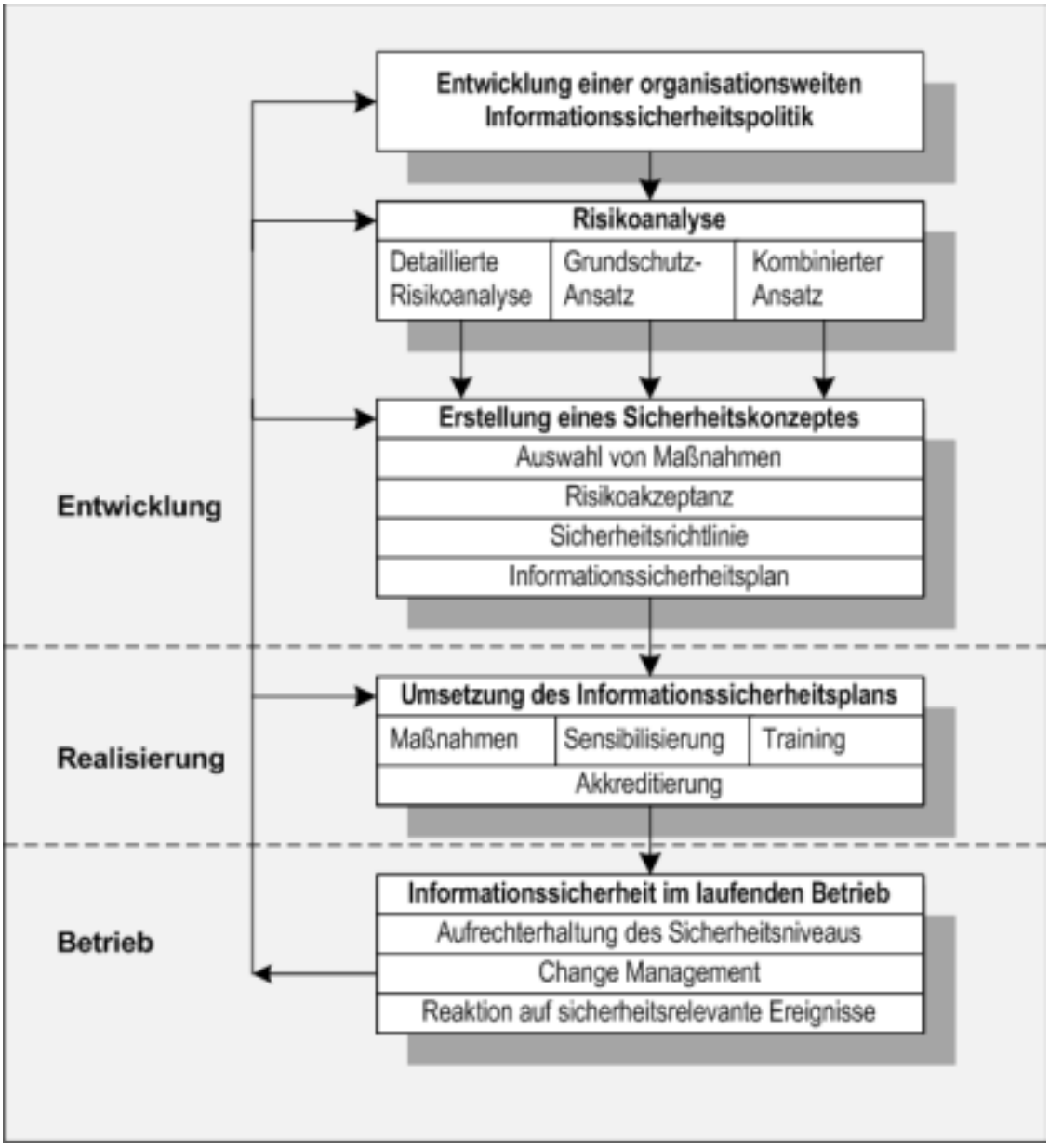

Abbildung 2.1: Aktivitäten im Rahmen des Informationssicherheitsmanagements

Informationssicherheitsmanagement umfasst damit die folgenden Schritte:

2.1.1 Entwicklung einer organisationsweiten Informationssicherheitspolitik

Als organisationsweite Informationssicherheitspolitik (Corporate Information Security Policy) bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksichtigung gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der Informationssicherheit festlegen.

Die organisationsweite Informationssicherheitspolitik (im Folgenden der Einfachheit halber als „Informationssicherheitspolitik“ bezeichnet) stellt ein langfristig orientiertes Grundlagendokument dar, auf dessen Basis die Informationssicherheit einer Organisation aufgebaut wird. Details zu Sicherheitsmaßnahmen und deren Umsetzung sind nicht Bestandteil der organisationsweiten Informationssicherheitspolitik, sondern sind im Rahmen einzelner systemspezifischer Sicherheitsrichtlinien zu behandeln.

Die Informationssicherheitspolitik ist eingebettet in eine Hierarchie von Regelungen und Leitlinien. Abhängig vom IT-Konzept und den Sicherheitsanforderungen kann es auch notwendig werden, eine Hierarchie von Informationssicherheitspolitiken für verschiedene Organisationseinheiten (etwa Abteilungen, nachgeordnete Dienststellen, …) zu erstellen.

2.1.2 Risikoanalyse

Eine wesentliche Aufgabe des Informationssicherheitsmanagements ist das Erkennen und Einschätzen von Sicherheitsrisiken und deren Reduktion auf ein tragbares Maß. Dieses „Informationsrisikomanagement“ oder auch „Informationssicherheitsrisikomanagement“ sollte Teil des generellen Risikomanagements einer Organisation und mit der dort gewählten Vorgehensweise kompatibel sein.

Aus Gründen der besseren Lesbarkeit wird im Folgenden, wenn nicht explizit anders erwähnt, der Begriff „Risiko“ stets im Sinne von „Informationssicherheitsrisiko“ verwendet, ebenso Risikoanalyse und Risikomanagement im Sinne von Informationssicherheitsrisikoanalyse und –management. Im Rahmen des vorliegenden Handbuchs werden drei Risikoanalysestrategien behandelt (siehe 5.1 Risikoanalyse): Detaillierte Risikoanalyse, Grundschutzansatz und Kombinierter Ansatz. Die Festlegung einer geeigneten Risikoanalysestrategie sollte im Rahmen der Informationssicherheitspolitik erfolgen, um ein organisationsweit einheitliches Vorgehen zu gewährleisten.

2.1.3 Erstellung eines Sicherheitskonzeptes

Abhängig von den Ergebnissen der Risikoanalyse werden in einem nächsten Schritt im Zuge der 5.2 Risikobehandlung Maßnahmen ausgewählt, die die Risiken auf ein definiertes und beherrschbares Maß reduzieren sollen. Im Anschluss daran ist das verbleibende Restrisiko zu ermitteln und zu prüfen, ob dieses für die Organisation tragbar ist oder weitere Maßnahmen zur Risikoreduktion erforderlich sind.

Für wichtige IT-Systeme und Anwendungen wird die Erstellung eigener Sicherheitsrichtlinien (auch als „IT-Systemsicherheitspolitiken“ bezeichnet) empfohlen. Diese sollen die grundlegenden Leitlinien zur Sicherheit eines konkreten IT-Systems bzw. einer Anwendung vorgeben sowie konkrete Sicherheitsmaßnahmen und ihre Umsetzung beschreiben. Die Sicherheitsrichtlinien müssen mit der organisationsweiten Informationssicherheitspolitik kompatibel sein.

In einem Informationssicherheitsplan werden alle kurz-, mittel- und langfristigen Aktionen festgehalten, die zur Umsetzung der ausgewählten Maßnahmen erforderlich sind.

Der Vorgang wird im Detail in 2.2 Erstellung von Sicherheitskonzepten behandelt.

2.1.4 Umsetzung des Informationssicherheitsplans

Bei der Implementierung der ausgewählten Sicherheitsmaßnahmen ist zu beachten, dass die meisten technischen Sicherheitsmaßnahmen ein geeignetes organisatorisches Umfeld brauchen, um vollständig wirksam zu sein. Unabdingbare Voraussetzung für eine erfolgreiche Umsetzung des Informationssicherheitsplans in der Praxis sind auch entsprechende Sensibilisierungs- und Schulungsmaßnahmen. Weiters ist festzulegen, wie die Effizienz und Effektivität der ausgewählten Sicherheitsmaßnahmen beurteilt werden kann. Dies erfolgt durch die Definition geeigneter Kennzahlen.

2.3 Umsetzung des Informationssicherheitsplanes behandelt diese Umsetzungsfragen.

2.1.5 Informationssicherheit im laufenden Betrieb

Umfassendes Informationssicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die Sicherheit im laufenden Betrieb aufrechtzuerhalten und gegebenenfalls veränderten Bedingungen anzupassen.

Zu den erforderlichen Follow-Up-Aktivitäten zählen (siehe 2.4 Informationssicherheit im laufenden Betrieb):

- Die Aufrechterhaltung des erreichten Sicherheitsniveaus
  Dies umfasst:
  - Wartung und administrativen Support von Sicherheitseinrichtungen
  - die Messung der Effektivität der ausgewählten Sicherheitsmaßnahmen anhand definierter Kennzahlen (*Information Security Measurement*)
  - die Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (*Security Compliance Checking*) sowie
  - die fortlaufende Überwachung der IT-Systeme (*Monitoring*)
- umfassendes Change-Management
- eine angemessene Reaktion auf sicherheitsrelevante Ereignisse (*Incident Handling*)

2.2 Erstellung von Sicherheitskonzepten

Ausgehend von den in der Risikoanalyse (siehe 5.1 Risikoanalyse) ermittelten Sicherheitsanforderungen wird ein Sicherheitskonzept erstellt. Dies erfolgt durch die Auswahl geeigneter Maßnahmen, die die Risiken auf ein akzeptables Maß reduzieren und unter dem Gesichtspunkt von Kosten und Nutzen eine optimale Lösung darstellen. Diese Bewertung und Verarbeitung der Ergebnisse einer Risikoanalyse wird auch unter dem Begriff Risikobehandlung zusammengefasst.

Ein Sicherheitskonzept enthält:

- die Beschreibung des Ausgangszustands einschließlich der bestehenden Risiken (Ergebnisse der vorangegangenen Risikoanalyse)
- die Festlegung der durchzuführenden Maßnahmen
- die Begründung der Auswahl unter Kosten/Nutzen-Aspekten und hinsichtlich des Zusammenwirkens der einzelnen Maßnahmen
- eine Abschätzung des Restrisikos sowie eine verbindliche Aussage über die Akzeptanz des verbleibenden Restrisikos
- die Festlegung der Verantwortlichkeiten für die Auswahl und Umsetzung der Maßnahmen sowie für die regelmäßige Überprüfung des Konzeptes
- eine Prioritäten-, Termin- und Ressourcenplanung für die Umsetzung

Die Erstellung eines Sicherheitskonzeptes erfolgt in vier Schritten:

- Schritt 1: Auswahl von Maßnahmen
- Schritt 2: Prüfung von Restrisiken und Risikoakzeptanz
- Schritt 3: Erstellung von Sicherheitsrichtlinien
- Schritt 4: Erstellung eines Informationssicherheitsplans

Diese vier Schritte werden in den folgenden Kapiteln näher beschrieben.

2.2.1 Auswahl von Maßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die die Sicherheit von Informationen und der sie verarbeitenden IT-Systeme erhöhen. Dies kann auf unterschiedliche Arten erreicht werden.

Sicherheitsmechanismen können:

- Risiken vermeiden
- Bedrohungen oder Schwachstellen verkleinern
- unerwünschte Ereignisse entdecken
- die Auswirkung eines unerwünschten Ereignisses eingrenzen
- Risiken überwälzen
- es möglich machen, einen früheren Zustand wiederherzustellen

2.2.1.1 Klassifikation von Sicherheitsmaßnahmen

Je nach Betrachtungsweise kann eine Klassifikation von Sicherheitsmaßnahmen hinsichtlich nachfolgender Kriterien getroffen werden.

Klassifikation nach Art der Maßnahmen

Dies ist die „klassische“ Einteilung der Sicherheitsmaßnahmen.

Man unterscheidet:

- (informations-)technische Maßnahmen
- bauliche Maßnahmen
- organisatorische Maßnahmen
- personelle Maßnahmen

Klassifikation nach Anwendungsbereichen

Man unterscheidet:

- Maßnahmen, die organisationsweit (oder in Teilen der Organisation) einzusetzen sind. Dazu gehören:
  - Etablierung eines ISMS-Prozesses und Erstellung von Informationssicherheitspolitiken
  - organisatorische Maßnahmen (z. B. Kontrolle von Betriebsmitteln, Dokumentation, Rollentrennung)

    - Überprüfung der IT-Sicherheitsmaßnahmen auf Übereinstimmung mit den Informationssicherheitspolitiken (Security Compliance Checking), Auditing
    - Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling)
    - personelle Maßnahmen (inkl. Schulung und Bildung von Sicherheitsbewusstsein)
    - bauliche Sicherheit und Infrastruktur
    - Notfallvorsorge
- Systemspezifische Maßnahmen. Die Auswahl systemspezifischer Maßnahmen hängt in hohem Maße vom Typ des zu schützenden IT-Systems ab. Man unterscheidet etwa:
    - Nicht-vernetzte Systeme (Stand-Alone-PCs)
    - Workstations in einem Netzwerk
    - Server in einem Netzwerk

Klassifikation nach Gefährdungen und Sicherheitsanforderungen

Ausgehend von den Grundbedrohungen gegen ein IT-System (Verlust der Vertraulichkeit, Integrität, Verfügbarkeit etc.) werden die typischen Gefährdungen ermittelt.

Man unterscheidet daher:

- Maßnahmen zur Gewährleistung der Vertraulichkeit (*confidentiality*)
- Maßnahmen zur Gewährleistung der Integrität (*integrity*)
- Maßnahmen zur Gewährleistung der Verfügbarkeit (*availability*)
- Maßnahmen zur Gewährleistung der Zurechenbarkeit (*accountability*)
- Maßnahmen zur Gewährleistung der Authentizität (*authenticity*)
- Maßnahmen zur Gewährleistung der Zuverlässigkeit (*reliability*)
- Maßnahmen zur Gewährleistung der Nichtwiderlegbarkeit (*non-repudiation*)

Wirksame Informationssicherheit verlangt im Allgemeinen eine Kombination von verschiedenen Sicherheitsmaßnahmen, wobei auf die Ausgewogenheit von technischen und nicht technischen Maßnahmen zu achten ist.

2.2.1.2 Ausgangsbasis für die Auswahl von Maßnahmen

Liste existierender bzw. geplanter Sicherheitsmaßnahmen:

Bei der Auswahl von Sicherheitsmaßnahmen zur Verminderung der Risiken wird vorausgesetzt, dass im vorhergehenden Schritt - der Risikoanalyse - die bereits existierenden Sicherheitsmaßnahmen aufgelistet wurden.

Bei einer Grundschutzanalyse werden die vorhandenen Maßnahmen im Rahmen eines Soll-Ist-Vergleiches (auch IT-Grundschutz-Check genannt, vgl. 5.1.2.3.3 IT-Grundschutz-Check) ermittelt. Im Fall einer detaillierten Risikoanalyse erfolgt dies im Rahmen der „Identifikation bestehender Schutzmaßnahmen“ (vgl. 5.1.3.1.6 Identifikation bestehender Sicherheitsmaßnahmen), die als Ergebnis eine Aufstellung aller existierenden oder bereits geplanten Schutzmaßnahmen mit Angaben über ihren Implementierungsstatus und ihren Einsatz liefern soll.

Ergebnisse der Risikobewertung:

> *Die Auswahl der Sicherheitsmaßnahmen, die die Risiken auf ein definiertes und beherrschbares Maß reduzieren, muss auf den Ergebnissen der Risikobewertung basieren.*

Diese Auswahl wird von einer Reihe von Faktoren beeinflusst:

- der Stärke der einzelnen Maßnahmen
- ihrer Benutzerfreundlichkeit und Transparenz für die AnwenderInnen
- der Art der Schutzfunktion (Verringerung von Bedrohungen, Erkennen von Verletzungen, …)

In der Regel stehen verschiedene mögliche Sicherheitsmaßnahmen zur Auswahl. Um die sowohl aus Sicherheits- als auch aus Wirtschaftlichkeitsüberlegungen effizienteste Lösung zu finden, kann im Einzelfall eine Kosten-/Nutzen-Analyse bzw. ein direkter Vergleich einzelner Sicherheitsmaßnahmen (*trade-off analysis*) notwendig sein.

2.2.1.3 Auswahl von Maßnahmen auf Basis einer detaillierten Risikoanalyse

> *Wurde eine detaillierte Risikoanalyse durchgeführt, so stehen für die Auswahl von geeigneten Sicherheitsmaßnahmen detailliertere und spezifischere Informationen zur Verfügung als im Fall einer Grundschutzanalyse. Je genauer und aufwändiger die Risikoanalyse durchgeführt wurde, desto qualifizierter ist i. Allg. die für den Auswahlprozess zur Verfügung stehende Information.*

In der Mehrzahl der Fälle wird es verschiedene Maßnahmen zur Erfüllung einer bestimmten Sicherheitsanforderung geben, die sich jedoch hinsichtlich ihrer Effizienz und ihrer Kosten unterscheiden. Umgekehrt kann eine Maßnahme gleichzeitig mehrere Sicherheitsanforderungen abdecken.

Welche der in Frage kommenden Maßnahmen tatsächlich ausgewählt und implementiert werden, hängt von den speziellen Umständen ab. Generell ist festzuhalten, dass Sicherheitsmaßnahmen einen oder mehrere der folgenden Aspekte abdecken können:

- Vorbeugung (präventive Maßnahmen)
- Aufdeckung (detektive Maßnahmen)
- Abschreckung
- Schadensbegrenzung
- Wiederherstellung eines früheren Zustandes
- Bildung von Sicherheitsbewusstsein
- Risikoüberwälzung

Welche dieser Eigenschaften notwendig bzw. wünschenswert ist, ist vom spezifischen Fall abhängig. In der Regel wird man Maßnahmen bevorzugen, die mehrere dieser Aspekte abdecken. Es ist aber auch darauf zu achten, dass die Gesamtheit der ausgewählten Maßnahmen ein ausgewogenes Verhältnis der einzelnen Aspekte aufweist, dass also nicht beispielsweise ausschließlich detektive oder ausschließlich präventive Maßnahmen zum Einsatz kommen.

2.2.1.4 Auswahl von Maßnahmen im Falle eines Grundschutzansatzes

Grundsätzlich ist die Auswahl von Sicherheitsmaßnahmen im Falle eines Grundschutzansatzes relativ einfach. In Maßnahmenkatalogen wird eine Reihe von Schutzmaßnahmen gegen die meisten üblichen Bedrohungen angeführt.

Die betreffenden Bedrohungen werden a priori, d. h. ohne weitere Risikoanalyse, als relevant für die durchführende Organisation angenommen. Die empfohlenen Maßnahmen werden mit den existierenden oder bereits geplanten Maßnahmen verglichen. Die noch nicht existierenden bzw. geplanten Maßnahmen werden in eine Liste von noch zu realisierenden Maßnahmen zusammengefasst.

Standardwerke zur Auswahl von Maßnahmen:

In diesem Sicherheitshandbuch werden die wichtigsten Grundschutzmaßnahmen für die öffentliche Verwaltung in Österreich angeführt. Alternativ kann auch auf andere bestehende Kataloge zurückgegriffen werden.

Eine sehr umfangreiche Sammlung von Grundschutzmaßnahmen, die kontinuierlich weiterentwickelt werden, findet sich etwa in den IT-Grundschutz-Standards und -Maßnahmenkatalogen des BSI (vgl. 5.1.2 Grundschutzansatz).

2.2.1.5 Auswahl von Maßnahmen im Falle eines kombinierten Risikoanalyseansatzes

Im Falle eines kombinierten Ansatzes werden zunächst anhand dieses Handbuchs oder eines Grundschutzkataloges wie z. B. dem des BSI entsprechende Schutzmaßnahmen ausgewählt und umgesetzt, die einerseits ein adäquates Sicherheitsniveau für Systeme der Schutzbedarfsklasse „niedrig bis mittel“ gewährleisten, andererseits auch für hochschutzbedürftige Systeme bereits ein gewisses Maß an Schutz bieten. Anschließend werden die noch fehlenden Sicherheitsmaßnahmen für IT-Systeme mit hohen bis sehr hohen Sicherheitsanforderungen ausgewählt.

2.2.1.6 Bewertung von Maßnahmen

Unabhängig von der verfolgten Strategie ist es in jedem Fall notwendig, die Auswirkungen der ausgewählten Maßnahmen zu analysieren. Damit soll gewährleistet werden, dass die zusätzlichen Maßnahmen mit dem IT-Gesamtkonzept und den bereits bestehenden Sicherheitsmaßnahmen verträglich sind, d. h. dass sie einander ergänzen und unterstützen und sich nicht etwa gegenseitig behindern oder in ihrer Wirkung schwächen.

In diesem Stadium ist auch die Einbeziehung der betroffenen BenutzerInnen zu empfehlen, da die Wirksamkeit von Sicherheitsmaßnahmen stark davon abhängt, in welchem Maß sie akzeptiert oder aber abgelehnt oder umgangen werden. Die Akzeptanz von Maßnahmen steigt, wenn ihre Notwendigkeit für die BenutzerInnen einsichtig ist.

Zur Bewertung von Sicherheitsmaßnahmen ist wie folgt vorzugehen:

- Erfassung aller Bedrohungen, gegen die die ausgewählten Maßnahmen wirken
- Beschreibung der Auswirkung der Einzelmaßnahmen
- Beschreibung des Zusammenwirkens der ausgewählten und der bereits vorhandenen Sicherheitsmaßnahmen
- Überprüfung, ob und inwieweit die Maßnahmen zu Behinderungen beim Betrieb des IT-Systems führen können
- Überprüfung der Vereinbarkeit der Maßnahmen mit geltenden rechtlichen Vorschriften und Richtlinien
- Bewertung, in welchem Ausmaß die Maßnahmen eine Reduktion der Risiken bewirken

Bevor die Maßnahmen umgesetzt werden, sollte die Leitungsebene entscheiden, ob die Kosten für die Realisierung der Maßnahmen im richtigen Verhältnis zur Reduzierung der Risiken stehen und ob die Risiken auf ein akzeptables Maß beschränkt werden.

2.2.1.7 Rahmenbedingungen

Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen sind stets auch Rahmenbedingungen (constraints) zu berücksichtigen, die entweder durch das Umfeld vorgegeben oder durch das Management festgelegt werden.

Beispiele für solche Rahmenbedingungen sind:

- Zeitliche Rahmenbedingungen
  Etwa: Wie schnell ist auf ein erkanntes Risiko zu reagieren? Wann kann/muss eine Maßnahme realisiert sein?
- Finanzielle Rahmenbedingungen
  Im Allgemeinen werden budgetäre Einschränkungen existieren. Die Kosten für Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum Wert der zu schützenden Objekte stehen.
- Umweltbedingungen
  Auch durch das Umfeld vorgegebene Rahmenbedingungen, wie etwa die Lage eines Gebäudes, klimatische Bedingungen und Platzangebot können die Auswahl von Sicherheitsmaßnahmen beeinflussen.
- Technische Rahmenbedingungen
  z. B. Kompatibilität von Hard- und Software

Weitere Einschränkungen können organisatorischer, personeller, gesetzlicher oder sozialer Natur sein.

Auch Rahmenbedingungen können im Laufe der Zeit, durch soziale Veränderungen oder durch Veränderungen im technischen oder organisatorischen Umfeld, einem Wandel unterliegen und sind daher regelmäßig zu überprüfen und zu hinterfragen.

2.2.2 Risikoakzeptanz

Absolute Sicherheit ist nicht erreichbar - auch nach Auswahl und Umsetzung aller angemessenen Sicherheitsmaßnahmen verbleibt i. Allg. ein Restrisiko. Um zu entscheiden, ob dieses für die betreffende Organisation tragbar ist oder weitere Maßnahmen zu veranlassen sind, ist wie folgt vorzugehen:

Schritt 1: Quantifizierung des Restrisikos

In diesem ersten Schritt ist das Restrisiko so exakt wie möglich zu ermitteln. Dabei bedient man sich am besten der Verfahren und Erkenntnisse aus der vorangegangenen Risikoanalyse.

Schritt 2: Bewertung der Restrisiken

Die verbleibenden Restrisiken sind als „akzeptabel“ oder „nicht akzeptabel“ zu klassifizieren. Die Entscheidungsgrundlage dafür sollte in der (organisationsweiten) Informationssicherheitspolitik festgelegt sein (vgl. 4.2.3 Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken sowie 5.2.1.4 Risikoakzeptanz). Akzeptable Restrisiken können in Kauf genommen werden, nicht akzeptable bedürfen einer weiteren Analyse.

Schritt 3: Entscheidung über nicht akzeptable Restrisiken

Die weitere Behandlung von nicht akzeptablen Restrisiken sollte stets eine Managemententscheidung sein. Es besteht die Möglichkeit, zu untersuchen, wie weit und mit welchen Kosten nicht akzeptable Restrisiken weiter verringert werden können, und zusätzliche, eventuell mit hohen Kosten verbundene Maßnahmen auszuwählen. Die Alternative dazu ist eine bewusste und dokumentierte Akzeptanz des erhöhten Restrisikos.

Schritt 4: Akzeptanz von außergewöhnlichen Restrisiken

Ist eine weitere Reduktion des Restrisikos nicht möglich, unwirtschaftlich oder aufgrund gegebener Rahmenbedingungen nicht wünschenswert, so besteht in begründeten Ausnahmefällen die Möglichkeit einer bewussten Akzeptanz dieses erhöhten Restrisikos. Das Vorgehen dabei und die Verantwortlichkeiten dafür sind in der Informationssicherheitspolitik festzulegen (vgl. 4.2.3 Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken sowie 5.2.4. Umgang mit Restrisiken).

2.2.3 Sicherheitsrichtlinien

Während das Sicherheitskonzept ganzheitlich Maßnahmen darstellt, um die Risiken auf ein definiertes und beherrschbares Maß zu bringen, sollen für jeweils spezifische Sicherheitsrichtlinien auf die einzelnen wichtigen Systeme eingehen.

2.2.3.1 Aufgaben und Ziele

Für alle komplexen oder stark verbreiteten IT-Systeme sollten spezifische Sicherheitsrichtlinien erarbeitet werden. Typische Beispiele sind etwa eine PC-Sicherheitsrichtlinie, eine Netzsicherheitsrichtlinie, eine Internetsicherheitsrichtlinie oder eine Richtlinie zum Einsatz mobiler Geräte.

2.2.3.2 Inhalte

Eine Sicherheitsrichtlinie sollte Aussagen zu den sicherheitsrelevanten Bereichen eines Systems treffen:

- Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Komponenten
- Definition der wichtigsten Ziele und Funktionalitäten des Systems
- Festlegung der Informationssicherheitsziele des Systems
- Abhängigkeit der Organisation vom betrachteten IT-System;
  dabei ist zu untersuchen, wie weit die Aufgabenerfüllung der Organisation durch eine Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität des Systems oder darauf verarbeiteter Information gefährdet wird.
- Investitionen in das System
  (Entwicklungs-, Beschaffungs- und Wartungskosten, Kosten für den laufenden Betrieb)
- Risikoanalysestrategie
- Werte, Bedrohungen und Schwachstellen lt. Risikoanalyse
- Sicherheitsrisiken
- Beschreibung der bestehenden und der noch zu realisierenden Sicherheitsmaßnahmen
- Gründe für die Auswahl der Maßnahmen
- Kostenschätzungen für die Realisierung und den laufenden Betrieb (Wartung) der Sicherheitsmaßnahmen
- Verantwortlichkeiten

2.2.3.3 Fortschreibung der Sicherheitsrichtlinien

Auch eine Sicherheitsrichtlinie stellt kein einmal erstelltes, unveränderbares Dokument dar, sondern ist regelmäßig auf Aktualität zu überprüfen und bei Bedarf entsprechend anzupassen.

Insbesondere ist es von Bedeutung, dass die Liste der existierenden bzw. noch umzusetzenden Sicherheitsmaßnahmen stets dem tatsächlich aktuellen Stand entspricht.

2.2.3.4 Verantwortlichkeiten

Die Verantwortlichkeiten für die Erstellung und Fortschreibung der Sicherheitsrichtlinien sind im Einzelnen in der Informationssicherheitspolitik festzulegen (vgl. dazu 6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit). Im Allgemeinen wird diese Verantwortung bei der/dem für das gegenständliche System zuständigen Informationssicherheitskoordinator im Bereich liegen, die/der sie mit der/dem CISO abstimmen wird. Letztere/r hat dafür Sorge zu tragen, dass die einzelnen Sicherheitsrichtlinien mit der organisationsweiten Informationssicherheitspolitik kompatibel sind und auch untereinander ein einheitliches, vergleichbares Niveau aufweisen.

2.2.4 Informationssicherheitspläne für jedes System

Ein Informationssicherheitsplan beschreibt, wie die ausgewählten Sicherheitsmaßnahmen umgesetzt werden. Er enthält eine Prioritäten- und Ressourcenplanung sowie einen Zeitplan für die Umsetzung der Maßnahmen.

Im Detail sind für jedes System zu erstellen:

- eine Liste der vorhandenen sowie eine Liste der noch zu implementierenden Sicherheitsmaßnahmen;
  für jede dieser Maßnahmen sollte eine Aussage über ihre Wirksamkeit sowie möglicherweise notwendige Verbesserungen oder Verstärkungen getroffen werden
- eine Prioritätenreihung für die Implementierung der ausgewählten Sicherheitsmaßnahmen bzw. die Verbesserung bestehender Maßnahmen
- eine Kosten- und Aufwandsschätzung für Implementierung und Wartung der Maßnahmen
- Detailplanung für die Implementierung
  Diese soll folgende Punkte umfassen:
  - Prioritäten
  - Zeitplan, abhängig von Prioritäten und Ressourcen
  - Budget
  - Verantwortlichkeiten
  - Schulungs- und Sensibilisierungsmaßnahmen
  - Test- und Abnahmeverfahren und -termine
  - Nachfolgeaktivitäten
- eine Bewertung des nach der Implementierung aller Maßnahmen zu erwartenden Restrisikos

Weiters sollte der Sicherheitsplan auch die Kontrollmechanismen festlegen, die den Fortschritt der Implementierung der ausgewählten Maßnahmen bewerten, und Möglichkeiten des Eingriffes bei Abweichungen vom vorgesehenen Prozess oder bei notwendigen Änderungen definieren.

2.2.5 Fortschreibung des Sicherheitskonzeptes

Das Sicherheitskonzept muss laufend fortgeschrieben werden, um an veränderte System- bzw. Umfeldeigenschaften angepasst zu bleiben.

Anlässe für eine neue Untersuchung und das Fortschreiben des Konzeptes können sein:

- Ablauf eines vorgeschriebenen oder vereinbarten Zeitraumes (z. B. jährliches Update)
- Eintritt von Ereignissen, die die Bedrohungslage verändern, wie etwa politische oder gesellschaftliche Entwicklungen oder das Bekanntwerden neuer Attacken
- Eintritt von Ereignissen, die die Werte verändern können, wie etwa die Änderungen von Organisationszielen oder Aufgabenbereichen, Änderungen am Markt oder die Einführung neuer Applikationen
- Ereignisse, die die Eintrittswahrscheinlichkeit von Bedrohungen verändern, wie etwa die Entwicklung neuer Techniken oder veränderte Einsatzbedingungen (Einsatzort, IT-Ausstattung, …)
- neue Möglichkeiten für Sicherheitsmaßnahmen, etwa aufgrund von Preisänderungen oder der Verfügbarkeit neuer Technologien

Voraussetzungen für eine effiziente und zielgerichtete Fortschreibung des Sicherheitskonzeptes sind:

- die laufende Überprüfung von Akzeptanz und Einhaltung der Sicherheitsmaßnahmen
- die Protokollierung von Schadensereignissen
- die Kontrolle der Wirksamkeit und Angemessenheit der Maßnahmen

Ob eine neuerliche Risikoanalyse erforderlich ist oder lediglich die Auswahl der Maßnahmen überarbeitet wird, hängt vom Ausmaß der eingetretenen Veränderungen ab.

2.3 Umsetzung des Informationssicherheitsplans

Die korrekte und effiziente Implementierung von Sicherheitsmaßnahmen und ihr zielgerichteter Einsatz hängen in hohem Maße von der Qualität des im vorangegangenen Schritt erstellten Informationssicherheitsplans ab. Dieser muss gut strukturiert, genau dokumentiert und den tatsächlichen Anforderungen der betroffenen Institution angepasst sein.

Bei der Umsetzung des Plans ist zu beachten, dass

- Verantwortlichkeiten rechtzeitig und eindeutig festgelegt werden,
- finanzielle und personelle Ressourcen rechtzeitig zugewiesen werden,
- die Maßnahmen korrekt umgesetzt werden,
- die Kosten sich in dem vorher abgeschätzten Rahmen halten,
- der Zeitplan eingehalten wird.

Gleichzeitig mit der Implementierung der Sicherheitsmaßnahmen sollten auch entsprechende Schulungs- und Sensibilisierungsmaßnahmen gesetzt werden, um die optimale Einhaltung und Akzeptanz der Maßnahmen bei den AnwenderInnen zu erreichen.

Als letzter Schritt der Umsetzung des Informationssicherheitsplans sind die implementierten Maßnahmen in ihrer tatsächlichen Einsatzumgebung auf ihre Auswirkungen zu testen und abzunehmen (Akkreditierung).

Es empfiehlt sich, die Umsetzung des Informationssicherheitsplans im Rahmen eines Projektes abzuwickeln.

2.3.1 Implementierung von Maßnahmen

Sobald der Informationssicherheitsplan erstellt und verabschiedet wurde, sind die einzelnen Maßnahmen zu implementieren, auf ihre Übereinstimmung mit der Sicherheitspolitik zu überprüfen (Security Compliance Checking) und auf Korrektheit und Vollständigkeit zu testen.

Dabei ist zu beachten, dass ein Teil der Maßnahmen systemspezifisch sein wird, ein anderer Teil aber organisationsweit einzusetzen ist (vgl. dazu auch 2.2.1 Auswahl von Maßnahmen).

Die Abstimmung der einzelnen systemspezifischen Informationssicherheitspläne für die Gesamtorganisation obliegt in der Regel der/dem CISO. Sie/er hat dafür Sorge zu tragen, dass

- die systemübergreifenden, organisationsweiten Maßnahmen vollständig und angemessen, sowie nicht redundant oder widersprüchlich sind
- die systemspezifischen Maßnahmen kompatibel sind und ein einheitliches, angemessenes Sicherheitsniveau haben

Besonderer Wert ist auf eine detaillierte, korrekte und aktuelle Dokumentation dieser Implementierungen zu legen.

Schritt 1: Implementierung der Sicherheitsmaßnahmen

> *Die Implementierung der ausgewählten Sicherheitsmaßnahmen hat anhand des Informationssicherheitsplans, entsprechend der vorgegebenen Zeitpläne und Prioritäten, zu erfolgen.*

Die Verantwortlichkeiten dafür sind im Detail festzulegen.

Schritt 2: Testplan und Tests

> *Tests sollen sicherstellen, dass die Implementierung korrekt durchgeführt und abgeschlossen wurde.*

Es wird empfohlen, für die Tests einen Testplan zu erstellen, der

- die Testmethoden
- die Testumgebung
- die Zeitpläne für die Durchführung der Tests

beinhaltet.

Die durchgeführten Tests sind im Detail zu beschreiben und die Ergebnisse in einem standardisierten Testbericht festzuhalten.

Abhängig von der speziellen Bedrohungslage und der Art der Maßnahmen kann die Durchführung von Penetrationstests erforderlich sein.

Schritt 3: Prüfung der Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

> *Security Compliance Checks sind sowohl im Rahmen der Implementierung der Maßnahmen als auch als wiederholte Aktivität zur Gewährleistung der Informationssicherheit im laufenden Betrieb (siehe dazu auch 18.1 Security Compliance Checking und Monitoring) durchzuführen.*

Dabei sind zu prüfen:

- die vollständige und korrekte Umsetzung der Sicherheitsmaßnahmen
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen
- die Einhaltung der organisatorischen Sicherheitsmaßnahmen im täglichen Betrieb

Dokumentation

Die Dokumentation der implementierten Maßnahmen stellt einen wichtigen Teil der gesamten Sicherheitsdokumentation dar und ist notwendige Voraussetzung für die Kontinuität und Konsistenz des Informationssicherheitsprozesses. Die wichtigsten Anforderungen an die Dokumentation sind:

- Aktualität:
  Alle Sicherheitsmaßnahmen sind stets auf dem aktuellen Stand der Realisierung zu beschreiben.
- Vollständigkeit
- Hoher Detaillierungsgrad:
  Die Sicherheitsmaßnahmen sind so detailliert zu beschreiben, dass zum einen eventuell bestehende Sicherheitslücken erkannt werden können, zum anderen ausreichend Information für einen korrekten und effizienten Einsatz der Maßnahmen zur Verfügung steht.
- Gewährleistung der Vertraulichkeit:
  Dokumentation über Sicherheitsmaßnahmen kann unter Umständen sehr vertrauliche Information enthalten und ist daher entsprechend zu schützen. So weit wie möglich sollte bei der Klassifizierung und Behandlung solcher Dokumente auf die Vorgaben im Rahmen der Informationssicherheitspolitik der Organisation zurückgegriffen werden (vgl. dazu 8.2 Klassifizierung von Informationen). Es kann im Einzelfall notwendig sein, weitere Verfahrensweisen zur Erstellung, Verteilung, Benutzung, Aufbewahrung und Vernichtung von sicherheitsrelevanter Dokumentation zu entwickeln. Diese Verfahrensweisen sind ebenfalls entsprechend zu dokumentieren.
- Konfigurations- und Integritätskontrolle:
  Es ist sicherzustellen, dass keine unautorisierten Änderungen der Dokumentation erfolgen, die eine - beabsichtigte oder unbeabsichtigte - Beeinträchtigung der implementierten Maßnahmen nach sich ziehen könnten.

2.3.2 Sensibilisierung (Security Awareness)

Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umsetzung der Richtlinien und Vorschriften zur Informationssicherheit zu erreichen. Um das Sicherheitsbewusstsein aller MitarbeiterInnen zu fördern und den Stellenwert der Informationssicherheit innerhalb einer Organisation zu betonen, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm erstellt werden, das zum Ziel hat, Informationssicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen.

Das Sensibilisierungsprogramm sollte systemübergreifend sein. Es ist Aufgabe der dafür verantwortlichen Person - dies wird in der Regel die/der CISO sein - die Anforderungen aus den einzelnen Teilbereichen und systemspezifische Anforderungen hier einfließen zu lassen und entsprechend zu koordinieren.

Das Sensibilisierungsprogramm sollte folgende Punkte umfassen:

- Information aller MitarbeiterInnen über die Informationssicherheitspolitik der Organisation. Im Rahmen einer Einführung sollten insbesondere folgende Punkte erläutert werden:
    - die Informationssicherheitsziele und -politik der Organisation sowie deren Erläuterung
    - die Bedeutung der Informationssicherheit für die Organisation
    - Organisation und Verantwortlichkeiten im Bereich der Informationssicherheit
    - die Risikoanalysestrategie
    - die Sicherheitsklassifizierung von Daten
    - ausgewählte Sicherheitsmaßnahmen (insbesondere solche, die für die gesamte Organisation Gültigkeit haben)
- die wichtigsten Ergebnisse der Risikoanalysen (Bedrohungen, Schwachstellen, Risiken, …)
- die Pläne zur Implementierung und Überprüfung der Sicherheitsmaßnahmen
- die Auswirkungen von sicherheitsrelevanten Ereignissen für einzelne Anwender und für die gesamte Institution
- die Notwendigkeit, Sicherheitsverstöße zu melden und zu untersuchen
- die Konsequenzen bei Nichteinhaltung von Sicherheitsvorgaben

Zur Sensibilisierung der MitarbeiterInnen können u. a. folgende Maßnahmen beitragen:

- regelmäßige Veranstaltungen zum Thema Informationssicherheit
- Publikationen
- schriftliche Festlegung der Berichtswege und Handlungsanweisungen im Falle eines vermuteten Sicherheitsproblems (z. B. Auftreten eines Virus, Angriff von außen („Hacker“), …)

Das Sensibilisierungsprogramm sollte alle MitarbeiterInnen der Institution auf ihre Verantwortlichkeit für Informationssicherheit hinweisen. Dabei ist insbesondere die Verantwortung des Managements für Informationssicherheit zu betonen („Informationssicherheit als Managementaufgabe“). Die organisationsweite Planung dieser Veranstaltungen sollte die/der CISO übernehmen. Gegebenenfalls liefern Informationssicherheitskoordinatoren im Bereich Informationen, wann und wo solche Veranstaltungen nötig sind.

Die Veranstaltungen zum Sensibilisierungsprogramm sollten in regelmäßigen Zeitabständen wiederholt werden, um das vorhandene Wissen aufzufrischen und neue MitarbeiterInnen zu informieren. Darüber hinaus sollte alle neuen, beförderten oder versetzten MitarbeiterInnen so weit in Fragen der Informationssicherheit geschult werden, wie es der neue Arbeitsplatz verlangt.

Das Sensibilisierungsprogramm ist regelmäßig auf seine Wirksamkeit und Aktualität zu überprüfen und laufend an Veränderungen in der Informationssicherheitspolitik sowie an neue Technologien anzupassen.

2.3.3 Schulung

Über das allgemeine Sensibilisierungsprogramm hinaus sind spezielle Schulungen zu Teilbereichen der Informationssicherheit erforderlich, wenn sich durch Sicherheitsmaßnahmen einschneidende Veränderungen, z. B. im Arbeitsablauf, ergeben.

Personen, die in besonderem Maße mit Informationssicherheit zu tun haben, sind speziell dafür auszubilden und zu schulen. Dazu zählen etwa:

- die/der CISO und die Informationssicherheitskoordinatoren im Bereich
- die Mitglieder des Informationssicherheitsmanagement-Teams
- MitarbeiterInnen, die zu als VERTRAULICH, GEHEIM oder STRENG GEHEIM eingestuften Informationen Zugang haben
- MitarbeiterInnen mit spezieller Verantwortung für die Systementwicklung (z. B. ProjektleiterInnen)
- MitarbeiterInnen mit spezieller Verantwortung für den Betrieb eines IT-Systems oder einer wichtigen Applikation (z. B. Applikationsverantwortliche)
- MitarbeiterInnen, die mit Aufgaben der IT-Sicherheitsverwaltung betraut sind (z. B. Vergabe von Zutritts-, Zugangs- und Zugriffsrechten)

Das Schulungsprogramm ist von jeder Organisation spezifisch für ihren eigenen Bedarf zu entwickeln. Besondere Betonung ist dabei auf die Schulung der korrekten Implementierung und Anwendung von Sicherheitsmaßnahmen zu legen. Typische Beispiele für die Themen, die im Rahmen von Schulungsveranstaltungen behandelt werden sollten, sind:

- Sicherheitspolitik und -infrastruktur:
  Rollen und Verantwortlichkeiten, Organisation des Informationssicherheitsmanagements, Behandlung von sicherheitsrelevanten Vorfällen, regelmäßige Überprüfung von Sicherheitsmaßnahmen und ähnliches
- Bauliche Sicherheit:
  Schutz von Gebäuden, Serverräumen, Büroräumen und Versorgungseinrichtungen mit besonderer Betonung der Verantwortung der einzelnen MitarbeiterInnen (z. B. Handhabung von Zutrittskontrollmaßnahmen, Brandschutz)
- Personelle Sicherheit
- Hardware- und Softwaresicherheit:
  Dazu gehören etwa Identifikation und Authentisierung, Berechtigungssysteme, Protokollierung, Wiederaufbereitung und Virenschutz.

- Netzwerksicherheit:
  Netzwerkinfrastruktur, LANs, Inter-/Intranets, Verschlüsselung, digitale Signaturen u. ä.
- Business Continuity-Planung

Schulungs- und Sensibilisierungsveranstaltungen zum Thema Informationssicherheit müssen zeitgerecht geplant und umgesetzt werden, um keine Sicherheitslücken durch mangelndes Wissen oder Sicherheitsbewusstsein entstehen zu lassen.

2.3.4 Akkreditierung

> *Unter Akkreditierung eines IT-Systems versteht man die durch eine unabhängige Instanz formal dokumentierte Sicherstellung, dass dieses den Anforderungen der Informationssicherheitspolitik und der Sicherheitsrichtlinien genügt.*

Wird ein IT-System akkreditiert, ist insbesondere darauf zu achten, dass seine Sicherheit

- in einer definierten Betriebsumgebung
- unter definierten Einsatzbedingungen
- für eine definierte vorgegebene Zeitspanne

gewährleistet ist.

Erst nach erfolgter Akkreditierung kann ein solches System - oder eine spezifische Anwendung davon - in Echtbetrieb gehen.

Techniken zur Akkreditierung sind:

- Prüfung der Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (*Security Compliance Checking*), vgl. auch 2.3.1 Implementierung von Maßnahmen und 2.4.3 Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)
- Tests
- Evaluation und Zertifizierung von Systemen

Änderungen der eingesetzten Sicherheitsmaßnahmen oder der Betriebsumgebung können eine neuerliche Akkreditierung des Systems erforderlich machen. Die Kriterien, wann eine Neuakkreditierung durchzuführen ist, sollten in den zugehörigen Sicherheitsrichtlinien festgelegt werden.

Wesentlich bei der Akkreditierung ist die Anwendung standardisierter und damit vergleichbarer Vorgehens- und Zustandsbeschreibungen sowie standardisierter Vorgaben für Erfüllung und Dokumentation.

2.4 Informationssicherheit im laufenden Betrieb

Umfassendes Informationssicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die Informationssicherheit im laufenden Betrieb aufrechtzuerhalten. Ein Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden. Weiters muss eine angemessene Reaktion auf alle sicherheitsrelevanten Änderungen sowie auf sicherheitsrelevante Ereignisse gewährleistet sein.

Ziel aller Follow-Up-Aktivitäten ist es, das erreichte Sicherheitsniveau zu erhalten bzw. weiter zu erhöhen. Verschlechterungen der Wirksamkeit von Sicherheitsmaßnahmen - sei es durch eine Veränderung der Bedrohungslage oder durch falsche Verwendung der implementierten Sicherheitsmaßnahmen - sollen erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

2.4.1 Aufrechterhaltung des erreichten Sicherheitsniveaus

Das nach der Umsetzung des Informationssicherheitsplans erreichte Sicherheitsniveau lässt sich nur dann aufrechterhalten, wenn Support, Compliance und Monitoring sichergestellt sind:

- Wartung und administrativer Support der Sicherheitseinrichtungen müssen gewährleistet sein,
- die realisierten Maßnahmen müssen regelmäßig auf ihre Übereinstimmung mit der Informationssicherheitspolitik geprüft werden (*Security Compliance Checking*)
- und die IT-Systeme fortlaufend überwacht werden (*Monitoring*).

Die Verantwortlichkeiten für diese Aktivitäten müssen im Rahmen der organisationsweiten Informationssicherheitspolitik bzw. in den einzelnen Sicherheitsrichtlinien detailliert festgelegt werden. Generell gilt auch hier, dass die Verantwortung für systemspezifische Maßnahmen bei den einzelnen Informationssicherheitskoordinatoren im Bereich - soweit definiert - liegen sollte, die Verantwortung für organisationsweite Sicherheitsmaßnahmen sowie die Gesamtverantwortung bei der/dem CISO.

Von besonderer Wichtigkeit für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen MitarbeiterInnen für Fragen der Informationssicherheit (vgl. dazu auch 2.3.2 Sensibilisierung (Security Awareness)).

2.4.2 Wartung und administrativer Support von Sicherheitseinrichtungen

Viele Sicherheitsmaßnahmen erfordern zur Gewährleistung ihrer einwandfreien Funktionsfähigkeit Wartung und administrativen Support. Zu diesen Aufgaben zählen etwa die regelmäßige Auswertung und Archivierung von Protokollen, Backup und Restore sowie die Wartung von sicherheitsrelevanten Komponenten, die Überprüfung der Parametereinstellungen und eventueller Rechte auf mögliche nichtautorisierte Änderungen, die Reinitialisierung von Startwerten oder Zählern sowie Updates der Sicherheitssoftware, wenn verfügbar (besonders, aber nicht ausschließlich, im Bereich Virenschutz).

Alle Wartungs- und Supportaktivitäten sollten nach einem detailliert festgelegten Plan erfolgen und regelmäßig durchgeführt werden.

Die Wartung von Sicherheitseinrichtungen hat in Abstimmung mit den Verträgen, die mit den Lieferfirmen geschlossen wurden, zu erfolgen und darf nur durch dafür autorisierte Personen vorgenommen werden.

Die Kosten für Wartungs- und Supportaufgaben können im Einzelfall beträchtlich sein und sollten daher bereits bei der Auswahl der Sicherheitsmaßnahmen bekannt sein und in den Entscheidungsprozess mit einfließen.

Um die Aufrechterhaltung eines einmal erreichten Sicherheitsniveaus zu gewährleisten, ist sicherzustellen, dass

- die erforderlichen finanziellen und personellen Ressourcen zur Wartung von Sicherheitseinrichtungen zur Verfügung stehen
- organisatorische Regelungen existieren, die die Aufrechterhaltung der Informationssicherheitsmaßnahmen im laufenden Betrieb ermöglichen und unterstützen
- die Verantwortungen im laufenden Betrieb klar zugewiesen werden
- die Maßnahmen regelmäßig daraufhin geprüft werden, ob sie wie beabsichtigt funktionieren
- Maßnahmen verstärkt werden, falls sich neue Schwachstellen zeigen

Alle Wartungs- und Supportaktivitäten im Sicherheitsbereich sollten protokolliert werden. Der regelmäßigen Auswertung dieser Protokolle kommt besondere Bedeutung für die gesamte Informationssicherheit zu.

2.4.3 Überprüfung von Maßnahmen auf Übereinstimmung mit der Informationssicherheitspolitik (Security Compliance Checking)

Zielsetzung

> *Zur Gewährleistung eines angemessenen und gleich bleibenden Sicherheitsniveaus ist dafür Sorge zu tragen, dass alle Maßnahmen so eingesetzt werden, wie es im Sicherheitskonzept und im Informationssicherheitsplan vorgesehen ist. Dies muss für alle IT-Systeme, -Projekte und Applikationen sowohl während der Planungsphase als auch im laufenden Betrieb und letztlich auch bei der Außerbetriebnahme sichergestellt sein.*

Dabei ist zu prüfen, ob

- die Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen gewährleistet ist (Stichproben!)
- die organisatorischen Sicherheitsvorgaben im täglichen Betrieb eingehalten und akzeptiert werden

Weiters sind die getroffenen Maßnahmen regelmäßig auf Übereinstimmung mit gesetzlichen und betrieblichen Vorgaben zu überprüfen.

Die Prüfungen können durch externe oder interne AuditorInnen durchgeführt werden und sollten soweit möglich auf standardisierten Tests und Checklisten basieren.

Zeitpunkte

Security Compliance Checks sollten zu folgenden Zeitpunkten bzw. bei Eintreten folgender Ereignisse durchgeführt werden:

- für neue IT-Systeme oder relevante neue Anwendungen:
  nach der Implementierung (vgl. dazu auch 18.1 Security Compliance Checking und Monitoring)
- für bereits in Betrieb befindliche IT-Systeme oder Applikationen:
  nach einer bestimmten, in den Sicherheitsrichtlinien vorzugebenden Zeitspanne (z. B. jährlich) sowie bei signifikanten Änderungen.

2.4.4 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Monitoring ist eine laufende Aktivität mit dem Ziel, zu überprüfen, ob das IT-System, seine BenutzerInnen und die Systemumgebung das im Informationssicherheitsplan festgelegte Sicherheitsniveau beibehalten. Dazu wird ein Plan für eine kontinuierliche Überwachung der IT-Systeme im täglichen Betrieb erstellt.

Wo technisch möglich und sinnvoll, sollte das Monitoring durch die Ermittlung von Kennzahlen unterstützt werden, die eine rasche und einfache Erkennung von Abweichungen von den Sollvorgaben ermöglichen. Solche Kennzahlen können beispielsweise die Systemverfügbarkeit, die Zahl der Hacking-Versuche über Internet oder die Wirksamkeit des Passwortmechanismus betreffen.

Alle Änderungen der potenziellen Bedrohungen, Schwachstellen, zu schützenden Werte und Sicherheitsmaßnahmen können möglicherweise signifikante Auswirkungen auf das Gesamtrisiko haben. Aus diesem Grund ist eine fortlaufende Überwachung folgender Bereiche erforderlich:

- Wert der zu schützenden Objekte:
  Sowohl die Werte von Objekten als auch, daraus resultierend, die Sicherheitsanforderungen an das Gesamtsystem können im Laufe des Lebenszyklus eines IT-Projektes oder -Systems erheblichen Änderungen unterliegen. Mögliche Gründe dafür sind eine Änderung der IT-Sicherheitsziele, neue Applikationen oder die Verarbeitung von Daten einer höheren Sicherheitsklasse auf existierenden Systemen oder Änderungen in der Hardwareausstattung.
- Bedrohungen und Schwachstellen:
  Organisatorisch oder technologisch (hier insbesondere durch neue Technologien in der Außenwelt) bedingt können sowohl die Wahrscheinlichkeit des Eintritts einer Bedrohung als auch die potenzielle Schadenshöhe im Laufe der Zeit starken Änderungen unterliegen und sind daher regelmäßig zu evaluieren. Neue potenzielle Schwachstellen sind so früh wie möglich zu erkennen und abzusichern.
- Sicherheitsmaßnahmen:
  Die Wirksamkeit der implementierten Sicherheitsmaßnahmen ist laufend zu überprüfen. Es ist sicherzustellen, dass sie einen angemessenen und den Vorgaben der Sicherheitsrichtlinien entsprechenden Schutz bieten. Änderungen in den Werten der bedrohten Objekte, den Bedrohungen und den Schwachstellen, aber auch durch den Einsatz neuer Technologien, können die Wirksamkeit der Sicherheitsmaßnahmen nachhaltig beeinflussen.

Durch ein kontinuierliches Monitoring soll die Leitung der Institution ein klares Bild darüber bekommen, was durch die Sicherheitsmaßnahmen erreicht wurde (Soll-/Ist-Vergleich), ob die Ergebnisse den Sicherheitsanforderungen der Institution genügen sowie über den Erfolg einzelner spezifischer Aktivitäten zur Informationssicherheit.

Werden im Rahmen des kontinuierlichen Monitorings signifikante Abweichungen des tatsächlichen Risikos von dem im Sicherheitskonzept festgelegten akzeptablen Restrisiko festgestellt, so sind entsprechende Gegenmaßnahmen zu setzen.

3 Managementverantwortung und Aufgaben beim ISMS

Zur Verantwortung der Managementebene gehört neben der Erreichung der geschäftlichen wie unternehmenspolitischen Ziele auch der angemessene Umgang mit Risiken. Sie müssen so früh wie möglich erkannt, eingeschätzt, bewertet und durch Setzen geeigneter und nachhaltiger Maßnahmen auf einen minimalen und akzeptierten Rest reduziert werden. Wegen der immer höheren Abhängigkeit von Information gilt dies besonders für Risiken aus fehlender oder mangelhafter Informationssicherheit.

3.1 Verantwortung der Managementebene

3.1.1 Generelle Managementaufgaben beim ISMS

Es ist eine Managementverantwortung, einen systematischen und dauerhaften Sicherheitsmanagementprozess zu etablieren, zu steuern und zu kontrollieren. Wird ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet, so ist es zu planen, zu implementieren, zu betreiben sowie zu kontrollieren und zu verbessern.

Dies bedeutet, dass die Managementebene für die Umsetzung folgender Aufgaben zu sorgen hat:

- Erarbeitung einer Sicherheitspolitik und Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung
- Erarbeitung der Sicherheitsziele und Detailaufgaben des ISMS
- Benennung von Rollen und verantwortlichen Personen (auch bei Bestellung externer Personen, wenn die Besetzung mit internem Personal nicht möglich ist)
- Darstellung, Einschätzung, Bewertung der Risiken, Festlegung von Kriterien für akzeptable Restrisiken
- Veranlassen des Aufbaus einer geeigneten Organisationsstruktur für Informationssicherheit
- Schaffung von Awareness (Bewusstsein) für die Bedeutung und den Nutzen eines angemessenen Informationssicherheitsniveaus bzw. des ISMS
- Schaffung von Awareness (Bewusstsein) und Motivation für die Notwendigkeit der Einhaltung der Sicherheitsregeln
- Schaffung von Awareness (Bewusstsein) und Motivation, über Schwachstellen und Sicherheitsvorfälle zu informieren und Verbesserungen vorzuschlagen

- Bereitstellung ausreichender finanzieller und personeller Ressourcen für Einrichtung und dauerhaften Betrieb des ISMS sowie der Sicherheitsmaßnahmen
- Durchführung von Audits und Management-Reviews im Rahmen des ISMS
- Herbeiführung von Entscheidungen über Verbesserungsvorschläge, im positiven Fall jeweils auch Sicherstellung von deren Umsetzung

Wie der Sicherheitsprozess organisiert wird, hängt zum einen von der Abgrenzung und zum anderen von seiner Komplexität ab, diese wiederum von Größe und Aufgaben der Organisation bzw. dem abgegrenzten Anwendungsbereich für das Sicherheitsmanagement. Sehr kleine Organisationen werden fallweise unter der Leitung des Geschäftsführers/der Geschäftsführerin punktuell externe Berater heranziehen, bei größeren Einheiten wird sich ein Mitglied der Managementebene persönlich um das ISMS kümmern bzw. wird ein/e Sicherheitsbeauftragte/r oder mehrere Sicherheitsbeauftragte benannt, welche mit Sicherheitsaufgaben betraut werden und diese ausschließlich oder zusätzlich zu anderen Aufgaben ausüben. Dies kann auch - etwa bei großen Organisationen oder solchen, für die Sicherheit zum Geschäftsmodell gehört - im Rahmen einer eigenen Sicherheitsorganisation zur Adressierung relevanter Gefährdungen erfolgen.

Relevante Gefährdungen sind:

- Fehlende persönliche Verantwortung im Sicherheitsprozess
- Mangelnde Unterstützung durch die Institutionsleitung
- Unzureichende strategische und konzeptionelle Vorgaben
- Unzureichende oder fehlgeleitete Investitionen
- Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen
- Fehlende Aktualisierung im Sicherheitsprozess
- Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
- Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen
- Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Unbeschadet davon bleibt die Gesamtverantwortung jedoch immer bei der Managementebene (bzw. Leitung). Sie kann diese Verantwortung allerdings nur dann effizient wahrnehmen, wenn sie stetig mit den essentiellen Informationen versorgt wird (analog dazu, dass sie mit Geschäftskennzahlen versorgt werden muss):

- Sicherheitsanforderungen, die sich aus gesetzlichen oder vertraglichen Verpflichtungen ableiten
- Aktuelle Sicherheitsrisiken mitsamt ihren möglichen - auch finanziellen - Auswirkungen, sowie ihre voraussichtliche Entwicklung
- Aufgetretene Schwachstellen oder Sicherheitsvorfälle

- Auswirkungen von tatsächlichen oder potenziellen Sicherheitsvorfällen auf kritische Geschäftsprozesse
- Potenzielle Gefährdungen aus veränderten Rahmenbedingungen und zukünftigen Entwicklungen
- Brauchbare Vorgehensweisen zur Informationssicherheit aus allgemeinen oder branchenüblichen Standards, vergleichbaren Organisationen, Arbeitsgruppen

Es muss laufend überprüft werden, ob und welche Sicherheitsmaßnahmen bzw. Verfahren des ISMS noch wirksam bzw. angemessen sind. Aus diesen Informationen sind von der Managementebene laufend Schlussfolgerungen zu ziehen und Entscheidungen zu treffen: welche Schwachstellen behoben wurden, ob und welche Sicherheitsmaßnahmen zu adaptieren sind und welche Verbesserungsmöglichkeiten umgesetzt werden.

Die Managementebene hat die Aufgabe, die MitarbeiterInnen zur aktiven Mitwirkung am Sicherheitsprozess zu motivieren und für diesbezüglich ausreichende Ausbildungs- und Awarenessmaßnahmen zu sorgen. Nur wenn der Sinn von Sicherheitsmaßnahmen bzw. -vorgaben und -anweisungen verstanden wird, werden diese auch gelebt und Informationen über Schwachstellen gegeben bzw. Verbesserungsvorschläge gemacht. Werden die AnwenderInnen in die Planung und Umsetzung von Maßnahmen einbezogen, werden sie auch von sich aus Ideen einbringen und die Tauglichkeit von Sicherheitsmaßnahmen aus Sicht der täglichen Praxis beurteilen.

Grenzen der Sicherheit:

- Es muss klar sein, dass Sicherheitsmaßnahmen - oft erhebliche - Kosten verursachen. Diesen sind jene gegenüberstellen, die als Folge eines schweren Sicherheitsvorfalls anfallen würden.
- Es muss ebenso klar sein, dass es keine absolute Sicherheit geben kann, sondern nur ein akzeptiertes Restrisiko.
- Es können Verkettungen von Vorfällen auftreten, die niemand vorhersagen kann und die ein höheres Schadenspotenzial als das akzeptierte Restrisiko nach sich ziehen.

Daher macht es Sinn, die Sicherheitsziele so zu definieren, dass sie zwar die Risiken auf das akzeptierte Maß senken, aber mit vertretbarem personellen, zeitlichen und finanziellen Aufwand erreicht werden können. Eine „starke“ Sicherheitsmaßnahme, die nie fertig wird, ist gar keine.

[Quelle: BSI Standard 200-2, Grundschutz-Kompendium ISMS.1]

3.2 Ressourcenmanagement

3.2.1 Bereitstellung von Ressourcen

Aufwand und Nutzen bei der Informationssicherheit

> *Ein angestrebtes Sicherheitsniveau ist nur dann sinnvoll, wenn es sich wirtschaftlich vertreten lässt und mit den verfügbaren personellen, zeitlichen und finanziellen Ressourcen auch erreicht werden kann. Ist das nicht möglich, dann müssen die Sicherheitsstrategie oder die Geschäftsprozesse bzw. die ihnen zugehörige Informationsverarbeitung geändert werden.*

Ab einem bestimmten Niveau rechnet sich der steigende Aufwand für angestrebte noch höhere Sicherheitsniveaus nicht mehr, da der tatsächliche Gewinn an Sicherheit immer geringer wird, bis er gar nicht mehr zunimmt.

Weit verbreitet ist die Ansicht, dass sich Informationssicherheit - insbesondere IT-Sicherheit - vor allem durch technische Maßnahmen bewerkstelligen lässt. Die Erfahrung zeigt allerdings, dass personelle Ressourcen und geeignete - oft sehr einfache - organisatorische Maßnahmen in vielen Fällen am effektivsten sind. Selbstverständlich ist Sicherheitstechnik eine wichtige Lösung und häufig unentbehrlich, aber nur innerhalb eines geeigneten organisatorischen Rahmens und bedient von qualifizierten Menschen.

Ressourcen für die Organisation

> *Erfahrungsgemäß ist die Benennung eines CISO eine sehr effiziente Sicherheitsmaßnahme, bei der die Anzahl an Sicherheitsvorfällen signifikant zurückgeht. Ihm/ihr muss allerdings ausreichend Zeit für die diesbezügliche Tätigkeit zugestanden werden. Ein CISO muss aber nicht jede Aufgabe selbst operativ abwickeln, sondern kann Aufgaben an das Informationssicherheitsmanagement-Team delegieren.*

Daher ist es in kleineren Organisationen eher möglich, dass er/sie die Sicherheitsaufgaben neben den eigentlichen Tätigkeiten ausübt. Größere Organisationen oder solche mit hohen Ansprüchen an Informationssicherheit, werden entweder hauptamtliche CISOs beschäftigen oder IS-Management-Teams aus mehreren MitarbeiterInnen zusammenstellen, welche dies neben ihren eigentlichen Aufgaben wahrnehmen können. Für Ad-hoc-Beratungen, Überprüfungen oder Implementierungen kann es sich auch für kleine Organisationen lohnen, kurzfristig externe Sicherheitsexperten heranzuziehen, gerade dann, wenn ein Mangel an Zeit oder der entsprechenden Expertise besteht. In einem solchen Fall muss auf den Schutz der Informationen gegenüber Externen geachtet werden (siehe dazu 13.2.1 Richtlinien beim Datenaustausch mit Dritten).

Ressourcen für die Einrichtung des ISMS: IS-Management-Team

Die sorgfältige Einrichtung und Planung des ISMS bedeutet einen erheblichen Zeit- und Arbeitsaufwand für alle mit der Informationssicherheit befassten MitarbeiterInnen, der dennoch in einem eher straffen Terminplan zu erledigen ist. Wenn möglich sollten diese als IS-Management-Team formiert und - zumindest ein Teil von ihnen - während dieser Zeit von ihren sonstigen Aufgaben so weit wie möglich freigestellt werden.

Mit einem solchen Team werden unterschiedliche Organisationseinheiten in den Sicherheitsprozess einbezogen und Kompetenzen gebündelt. Die Informationssicherheit wird dadurch schneller in allen Organisationseinheiten umgesetzt und es gibt weniger Konflikte.

Das IS-Management-Team kann sich etwa - je nach Größe und Art der Organisation - aus folgenden Bereichen zusammensetzen:

- Informationssicherheit
- Fachabteilungen
- Haustechnik
- Revision
- IT, Datenschutz
- Personal
- Betriebsrat
- Finanz/Controlling
- Rechtsabteilung

Für eine kontinuierliche Steuerung des Prozesses sollte ein solches IS-Management-Team regelmäßig zusammenkommen.

Ressourcen für Betrieb und Überprüfung

Ein reibungsloser IT-Betrieb ist zwar eine Voraussetzung für Informationssicherheit, in vielen Fällen aus Ressourcenmangel aber nicht gegeben. Überlastete IT-MitarbeiterInnen, mangelhaft gewartete IT-Einrichtungen, fehlende Ausbildung etc. sind Quellen für plötzlich auftretende Fehler, welche die ohnehin problematische Situation verschärfen. Zusätzlich kann es zu schleichender Demotivierung mit allen negativen Folgen führen.

Daher sollte sich die Managementebene immer wieder vom Ablauf des Betriebs und der Situation der MitarbeiterInnen überzeugen und bei Mängeln für deren rasche Behebung sorgen.

Weiters sind personelle, zeitliche und finanzielle Ressourcen erforderlich und bereitzustellen, um die Wirksamkeit und Eignung der Sicherheitsmaßnahmen systematisch überprüfen zu können. Dabei ist auch laufend zu bewerten:

- ob der Aufwand jeweils noch im Einklang zum Sicherheitsnutzen steht,
- welche Alternativen eingesetzt werden könnten,
- ob die verwendeten Sicherheitsmaßnahmen die zugehörigen Geschäftsprozesse noch unterstützen.

Schließlich sind noch Ressourcen bereitzustellen, um das ISMS selbst auf Konsistenz und Wirksamkeit zu überprüfen (interne/externe Audits, Management-Reviews) und ggf. Verbesserungen einzuleiten. Dies wird in der Regel von entsprechend ausgebildeten MitarbeiterInnen in Zusammenwirken mit der Managementebene durchgeführt.

[Quelle: BSI Standard 200-1]

3.2.2 Schulung und Awareness

Wirksame Informationssicherheitsmaßnahmen benötigen neben ihrer sachlichen Implementierung eine Sicherheitskultur der Organisation, ausgeprägtes Sicherheitsbewusstsein bei den MitarbeiterInnen und deren ausreichende und weiterentwickelte Qualifikation.

Dies ist ein langfristiger und kontinuierlicher Prozess mit vielschichtigen Effekten:

- Überzeugung aller MitarbeiterInnen, dass Informationssicherheit ein Erfolgsfaktor ist
- Überzeugung aller MitarbeiterInnen, dass und warum bestimmte Sicherheitsmaßnahmen notwendig und sinnvoll sind
- Wissen bei den MitarbeiternInnen über Erwartungen hinsichtlich Informationssicherheit und Sensibilisierung für Sicherheitsaspekte
- Wissen bei den MitarbeiternInnen, was sie in kritischen Situationen tun bzw. unterlassen sollen
- Ausreichende Kenntnisse und Fertigkeiten zur Durchführung ihrer Aufgaben
- Kenntnis der betrieblichen Abläufe und damit verbundener Regelungen
- Kenntnis der AnsprechpartnerInnen für Sicherheitsfragen oder -probleme
- Vorbeugung von Sicherheitsvorfällen und sorgsamer Umgang mit Informationen sowie mit der IT

Die Organisation wird ihre geschäftlichen, aber auch sicherheitsrelevanten Ziele wohl nur mit hinreichend ausgebildeten und informierten MitarbeiterInnen erreichen. Das beginnt selbstverständlich schon bei der Auswahl von BewerberInnen bei der Einstellung und setzt dafür genaue und aktuelle Job-Beschreibungen voraus.

Die mitgebrachten Kenntnisse und Erfahrungen decken jedoch nur einen Teil des Benötigten für die nunmehrige Tätigkeit ab und werden mit der Zeit weniger aktuell. Laufende Information, Schulung und positive Bewusstseinsbildung vermittelt Kompetenz und ermöglicht den MitarbeiterInnen, die Folgen und Auswirkungen ihrer Tätigkeit im beruflichen und privaten Umfeld einzuschätzen.

Gefährdungen:

Unzureichende Informationen und Kenntnisse können im Bereich der Informationssicherheit eine Reihe von Gefährdungen heraufbeschwören:

- Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten (unzureichende Kenntnis der Regelungen, unerlaubte Ausübung von Rechten, Fehlerhafte Nutzung oder Administration von IT-Systemen)
- Nichtbeachtung von Sicherheitsmaßnahmen
- Sorglosigkeit im Umgang mit Informationen
- Mangelhafte Akzeptanz von Informationssicherheit

Weiters kann aus unzureichender Information (etwa wenn dies als böse Absicht des Managements interpretiert wird) im Zusammenwirken mit stetiger Überlastung Frustration entstehen, was mitunter zu vorsätzlichen Handlungen führen kann:

- Unberechtigte IT-Nutzung
- Missbrauch von Benutzer- oder Administratorrechten
- Manipulation an Informationen oder Software
- Social Engineering
- Ausspähen von Informationen

Es muss daher im vitalen Interesse der Managementebene liegen, sich der Bedeutung von ausreichender Information, Schulung und Awareness für Informationssicherheit bei den MitarbeiterInnen bewusst zu sein und Schulungs- und Awarenessmaßnahmen nachhaltig zu unterstützen. Selbstverständlich gilt auch hier der Grundsatz der Angemessenheit: Schulungen sind kein Selbstzweck, sondern ein Mittel zur Erreichung der geschäftlichen und sicherheitspolitischen Ziele und unterliegen wie jede andere Maßnahme einer Kosten-/Nutzen Relation.

Schulungs- und Awarenessprogramm:

Optimalerweise wird für umfassende und angemessene Kompetenz ein Schulungs- und Awarenessprogramm aufgebaut und in Schritten durchlaufen. Damit werden Unterschiede im Wissenstand einzelner MitarbeiterInnen - abgesehen von ausgesprochenen Spezialisierungen - ausgeglichen.

Speziell kleine Organisationen werden sich jedoch mitunter auf das Aufspüren und Beheben individueller Kenntnislücken beschränken müssen, haben dafür meist mit geringerer Komplexität zu tun. Die generellen Anforderungen sind jedoch die gleichen wie bei größeren Einheiten.

Planung und Konzeption:

Am Beginn des Programms steht die sorgfältige Planung - diese zahlt sich wörtlich aus, da Schulungen, Seminare etc. erhebliche Kosten verursachen können und den MitarbeiterInnen erhebliche Zeit abverlangen, in der sie für ihre eigentlichen Aufgaben nicht zur Verfügung stehen.

- Lernziele definieren, messen und auswerten: Vor allem Sicherheitsziele der eigenen Organisation müssen vermittelt werden, aber auch Basiswissen zu Informationssicherheit und Fertigkeiten für Verhalten in kritischen Situationen. Diese Lernziele sollten gemessen und ausgewertet werden.
- Erfolgskriterien für das Schulungs- und Awarenessprogramm definieren inkl. deren Messung, soweit möglich.
- Zielgruppen für einzelne Schulungs- und Awarenessmaßnahmen definieren, da diese unterschiedliche Bedürfnisse aber auch Zeitressourcen haben sowie berücksichtigen von vertiefenden Schulungen für besonders exponierte Personen (etwa: Management, AdministratorInnen, Externe).
- Lernbedarf identifizieren: auf Basis bisheriger Kenntnisse, Spezialisierung (etwa: neue MitarbeiterInnen, Basiswissen, Spezialkenntnisse, neue Abläufe/Systeme).
- Lerninhalte festlegen: jedenfalls alle Regelungen und Verfahren für den jeweiligen Arbeitsplatz, inkl. Umfeld und Hintergründen. Hier besteht jedoch die Gefahr einer Überfrachtung, so dass dann aus Zeitmangel die Schulung gar nicht vollständig durchgeführt wird. Im IT-Bereich können Sicherheitsschulungen durchaus in IT-Schulungen integriert werden, sofern die TrainerInnen hinreichend qualifiziert sind und der Sicherheit hinreichend Platz eingeräumt wird.
- Lernmethoden und -medien auswählen: eine wesentliche Entscheidung ist, ob eigene MitarbeiterInnen die Schulungen durchführen oder externe TrainerInnen. Weiters ist zu klären, ob standardisierte Seminare („von der Stange“) ausreichen (dazu sind auch deren Termine zu berücksichtigen), ob und inwieweit individuelle Schulungen notwendig sind oder ob z. B. E-Learning eingesetzt werden kann.

Schulungs- und Awarenessprogramme, die bereits einmal durchgeführt wurden, sollten auf ihren Erfolg und ihre künftige Brauchbarkeit - auch für weitere Programme - untersucht werden. Weiters - vor allem bei E-Learning - muss auf potenzielle Sicherheitsrisiken durch die Schulungsmedien geachtet werden (etwa aktive Inhalte wie Java, Javascript, ActiveX) und ggf. darauf verzichtet oder nur dezidierte Internet-PCs dafür verwendet werden. Findet die Schulung in den eigenen Räumen statt, dann muss für die notwendige Infrastruktur (Konferenzraum, Projektor, Stromanschluss etc.) gesorgt werden.

Durchführung und Kontrolle:

Damit möglichst alle vorgesehenen MitarbeiterInnen effizient geschult werden, ist eine sorgfältige Terminplanung erforderlich. Die zu schulenden MitarbeiterInnen müssen für die Zeit der Schulung möglichst von ihren angestammten Aufgaben freigestellt werden.

Die Lerneinheiten sollten jeweils zeitlich so gestaltet werden, dass die Inhalte auch aufgenommen werden können. Wenn nicht anders möglich, muss ggf. auch Zeit für die Erledigung der wichtigsten Aufgaben verbleiben.

Im Fall externer TrainerInnen muss darauf geachtet werden, dass sie im Zuge der Schulung nicht Kenntnis über sensible Informationen erhalten.

Nach der Schulungs-/Awarenessmaßnahme sollte ihr Erfolg und ihre Effizienz überprüft werden:

- Wurden alle betroffenen MitarbeiterInnen erreicht?
- Wurden die Inhalte verstanden?
- Waren die MitarbeiterInnen mit der Schulungs-/Awarenessmaßnahmen zufrieden?
- Gibt es (sachlich begründeten) Bedarf für weitere Schulungen?
- Hat sich die Einstellung der MitarbeiterInnen gegenüber Sicherheitsmaßnahmen positiv geändert? Dies ist allerdings nicht einfach zu ermitteln, da es zu keinen missbräuchlichen Überwachungsaktionen kommen darf.

Methoden, um den Erfolg nachzuprüfen, können sein:

- Fragebögen mit Bewertungen der Teilnehmer
- Fragebögen mit Fragen aus dem gelernten Stoff
- Diskussionsmeeting Management/Sicherheitsbeauftragte/MitarbeiterInnen nach der Schulungs-/Awarenessmaßnahme

Dokumentation von Schulungs-/Awarenessmaßnahmen:

Am Schluss einer Aus- oder Weiterbildungsmaßnahme sollte jedem Teilnehmer/ jeder Teilnehmerin eine Teilnahmebestätigung übergeben werden, ggf. kann auch ein positives Absolvieren dargestellt werden. Die Organisation sollte für alle MitarbeiterInnen im Personalakt festhalten, welche Schulungs-/ Awarenessmaßnahmen absolviert wurden.

Flankierende Schulungs- und Awarenessmaßnahmen:

Abgesehen von „klassischen“ Schulungs-/Awarenessmaßnahmen bieten sich zur kontinuierlichen Weiterbildung an:

- Informationsforum zur Informationssicherheit im Intranet
- Anmeldebildschirm mit Sicherheitsinformationen resp. 1-2 Quizfragen
- Rundschreiben, E-Mails, Zeitschriften mit sicherheitsrelevanten Themen
- Mitarbeiterzeitung, Poster und Broschüren
- interne Informationsveranstaltungen
- externe Seminare, Messen und Konferenzen
- E-Learning-Programme
- Planspiele zur Informationssicherheit
- Diskussionsmeetings (Round-Tables, Kaminabende)

Flankierende Schulungs- und Awarenessmaßnahmen:

Vor dem Hintergrund ständig neuer Anwendungen, IT-Systemen, Bedrohungen, Schwachstellen und möglicher Abwehrmaßnahmen ist eine ständige Auffrischung und Erweiterung des Wissens über Informationssicherheit erforderlich.

Daher sollte das Schulungsangebot sowohl für neue wie auch für erfahrene MitarbeiterInnen in regelmäßigen Abständen Auffrischungs- und Ergänzungskurse vorsehen. Die Schulungsprogramme selbst müssen regelmäßig aktualisiert und an neue Gegebenheiten angepasst werden.

[Quelle: BSI ORP.3]

3.3 Interne ISMS Audits

Interne Audits dienen zur Überprüfung, ob Ziele, Vorgaben, Maßnahmen und Verfahren innerhalb der eigenen Organisation:

- die gesetzlichen und normativen Vorschriften erfüllen,
- nach wie vor geeignet sind, um die Informationssicherheitsziele zu erreichen,
- korrekt umgesetzt sind und von allen Beteiligten eingehalten werden,
- einwandfrei funktionieren und wirksam sind.

Interne Audits sind bei Akkreditierungen meist eine notwendige Vorleistung für extern durchgeführte Akkreditierungs- oder Zertifizierungsaudits. Weiterer Nutzen liegt im Erkennen von:

- Schulungs- und Informationsbedarf der Führungskräfte und MitarbeiterInnen
- Verbesserungspotenzial bei Geschäftsprozessen und Sicherheitsmaßnahmen
- Möglichkeiten zur Optimierung der Organisation

- sowie in der Motivation der MitarbeiterInnen, da sie ihre Gedanken im Rahmen des Audits einbringen können und sollen

3.3.1 Planung und Vorbereitung interner Audits

Interne Audits sollten einmal pro Jahr durchgeführt werden und dabei nicht in Zeiten hoher Arbeitsbelastungen (Systemumstellungen, Rechnungsabschlüsse etc.) oder reduzierter Ressourcen (Urlaubszeit) fallen.

Interne Audits können im Vergleich zu zeitlich begrenzteren externen Akkreditierungs- bzw. Zertifizierungsaudits wesentlich umfassender erfolgen, tiefer in die Themen eindringen und können jeweils nach und nach Teilbereiche der Organisation umfassen. Damit können Schwachstellen besser erkannt und zielgerichtete Verbesserungen eingeleitet werden.

Die Managementebene muss den Auditprozess initiieren und mittragen sowie dafür sorgen, dass den AuditorInnen und teilnehmenden MitarbeiterInnen ausreichend Zeit und Sachressourcen (Konferenzraum, PC) zur Verfügung gestellt werden. Das Audit sollte nach einem Auditplan verlaufen, welcher der Managementebene sowie allen Beteiligten bzw. Betroffenen vorab bekannt gegeben wird. Der Auditplan enthält eine konkrete Checkliste, nach der die AuditorInnen die Audit-Themen Punkt für Punkt durchgehen und die u. a. enthält:

- Datum
- Zeit
- Thema
- Teilnehmer
- Erledigungsvermerk

Anforderungen an die Durchführung des Audits und die Verantwortlichkeiten sind festzulegen und zu dokumentieren, ebenso die Anforderungen an die Ergebnisdokumentation. Werden im Zuge des Audits vertrauliche Dokumentationen benötigt, so ist für deren ausreichenden Schutz zu sorgen.

Bei der Planung des Auditprogramms ist zu priorisieren, welche Bedeutung die zu untersuchenden Bereiche haben und in welchem Status (Planung/Etablierung/Test/ produktiver Betrieb) sie sich befinden; ebenso müssen die Ergebnisse aus früheren Audits einfließen.

Anforderung an AuditorInnen:

Die Managementebene muss einen oder mehrere AuditorInnen benennen, an die allerdings Anforderungen zu stellen sind:

Objektivität und Unparteilichkeit:

- AuditorInnen dürfen nur Bereiche auditieren, in denen sie nicht selbst tätig sind
- bzw. für welche sie nicht verantwortlich sind

Fachliche Qualifikationen:

- ausreichende Schul- und Berufsausbildung um die Geschäftsprozesse und Sicherheitsmaßnahmen zu verstehen
- Kenntnis der relevanten Gesetze und Normen, inkl. für das Audit relevante Normen (z. B. ISO 19011)
- Kenntnis der Unternehmens- und Sicherheitsziele sowie der wesentlichen Abläufe und Prozesse
- Kenntnisse der wesentlichen Themen der Informationssicherheit
- Schulung um Audits durchführen zu können (Methodik, Fragetechnik, Analyse, Bewertung, Berichtswesen)

Persönliche Fähigkeiten:

- Klare und verständliche mündliche und schriftliche Ausdrucksweise
- Aktives Zuhören
- Ausdauer, Belastbarkeit, Festigkeit auch in Stresssituationen
- Einfühlungsvermögen zugleich mit Beharrlichkeit
- Erkennen von größeren Zusammenhängen und Konsequenzen aus Einzelinformationen

3.3.2 Durchführung interner Audits

AuditorInnen und Beteiligte aus den zu auditierenden Organisationseinheiten haben sich vorzubereiten (Auditplan, Programm, Checkliste, Handbücher, Systembeschreibungen, Sicherheitskonzept, …). Meist beginnt ein Audit mit einem Gespräch der AuditorInnen und maßgeblichen MitarbeiterInnen. Mitglieder der Managementebene sollten nach Möglichkeit anwesend sein.

Zunächst erklären die AuditorInnen die Zielsetzung des Audits, der vorläufige Zeitplan wird besprochen, vor allem wann welche MitarbeiterInnen zur Verfügung stehen sollen.

Detailüberprüfungen finden meist im Gespräch mit den jeweils befassten MitarbeiterInnen - wenn möglich - an deren Arbeitsplatz statt. Dabei werden die Unterlagen (Vorgaben, Systembeschreibungen, Dokumentationen, Arbeitsanweisungen) durchgegangen und Fragen gestellt/beantwortet. Es ist oft sinnvoll, mit aktuellen Themen zu beginnen. Es liegt an den AuditorInnen, ein konstruktives und positives Klima zu schaffen - etwa indem zu Ideen und Beiträgen für Verbesserungsmaßnahmen ermuntert wird und diese notiert werden. Damit

werden auch allfällige Ängste vor Notizen genommen. Werden Abweichungen von einer Vorgabe erkannt, so sollte nach weiteren Beispielen gefragt werden, um allfällige systematische Abweichungen aufzudecken. Diese sind relevant für Verbesserungsmaßnahmen: das Problem kann an der Einhaltung, aber auch an den Vorgaben liegen.

Inhaltliche Grundlage des internen Audits sind die Vorgaben (Gesetze, Normen, Geschäftsziele, Sicherheitspolitik, Sicherheitskonzept, …). Es ist zunächst zu hinterfragen:

- Sind die Vorgaben geeignet, die relevanten Gesetze einzuhalten und Normen zu erfüllen?
- Welche Vorgaben sind vorhanden? Sind sie den befassten Personen bekannt und werden sie verstanden?
- Sind die Vorgaben vollständig und klar formuliert?
- Gehen aus den Vorgaben die Verantwortlichkeiten und Zuständigkeiten hervor?
- Beschreiben die Vorgaben jeweils geschlossene Workflows (Eingabe/ Verarbeitung/Ausgabe-Ergebnis)?
- Gibt es Vorgaben zur Protokollierung von Abweichungen/Vorfällen?
- Wurden allfällige Verbesserungsmaßnahmen aus dem letzten Audit umgesetzt und wie?

Der nächste Fragenkomplex betrifft ihre Einhaltung:

- Welche Nachweise sind vorgesehen, um die Einhaltung kontrollieren und überprüfen zu können?
- Gibt es Vorgaben, die nicht angewendet werden?
- Gibt es umgekehrt durchgeführte Tätigkeiten, für die keine Vorgaben existieren?
- Wie exakt werden die Vorgaben bei der praktischen Tätigkeit eingehalten?
- Gab es Sicherheitsvorfälle, konnten solche anhand der Vorgaben behoben werden/musste improvisiert werden?
- Gab es Änderungen bei den Vorgaben aufgrund von Sicherheitsvorfällen?
- Werden die jeweiligen Tätigkeiten in der Praxis dokumentiert und wie (Arbeitsaufzeichnungen, Tagesprotokolle, …)?
- Welche dokumentierten Hinweise über die Wirksamkeit der Vorgaben / Maßnahmen gibt es (verhinderte Eindringversuche, erfolgte Behebung von Störungen, …)?
- Welche persönliche Meinung haben die befassten MitarbeiterInnen von den Vorgaben? Halten sie die Vorgaben für sinnvoll?
- Welche Verbesserungsmaßnahmen schlagen die MitarbeiterInnen vor?

Die Fragenkomplexe werden mit Hilfe der Checkliste durchgegangen. Diese dient aber nur als Leitfaden, situationsbezogen müssen ergänzende Fragen gestellt und beantwortet werden, wenn Vertiefung zum Verständnis notwendig wird oder sich ein Verdacht auf Abweichungen ergibt. Die Erkenntnisse für die AuditorInnen ergeben sich aus den Antworten in Relation mit den schriftlichen Unterlagen.

Schon bei der Frage-/Antwortdiskussion müssen die AuditorInnen auf Objektivität und Unparteilichkeit achten. Meinungsäußerungen, ob eine bestimmte Maßnahme gut oder weniger gut umgesetzt ist, bieten Feedback und können zu einer angeregteren Diskussion beitragen, sollten allerdings gezielt eingesetzt werden. Sinnvoll ist es dabei, nach den Gründen für entdeckte nicht eingehaltene Vorgaben zu fragen (nicht verstanden/Überlastung/mangelnde Information, …). AuditorInnen müssen allerdings speziell darauf achten, dass ihre Fragen stets zum Zweck des Audits und keinesfalls zu ihrer eigenen Weiterbildung gestellt werden.

Am Schluss der Durchführungsphase sollte wiederum ein Gespräch der AuditorInnen mit maßgeblichen MitarbeiterInnen und ManagementvertreterInnen stattfinden. Dabei wird den TeilnehmerInnen für ihre Mitwirkung gedankt und eine Vorschau auf das Ergebnis geboten:

- Vorläufige Erkenntnisse aus der Befragung und den Unterlagen
- Zeitpunkt und Art der Berichtslegung (Erkenntnisse, Empfehlungen)
- Allfällige Möglichkeiten zur Stellungnahme
- Termin für Schlussdokument und Schlusspräsentation

3.3.3 Ergebnis und Auswertung interner Audits

Die Erkenntnisse aus den Befragungen werden den einzelnen Vorgaben und Beschreibungen zugeordnet und von den AuditorInnen analysiert. Dabei ist auf Objektivität zu achten, etwa bei den subjektiv empfundenen Gründen für Abweichungen.

Beispiele für Erkenntnisse, welche Maßnahmen nach sich ziehen müssen:

- Wesentliche Vorgaben für Arbeitsabläufe fehlen, sind falsch oder mangelhaft.
- Verantwortlichkeiten oder Zuständigkeiten für Prozesse fehlen oder sind falsch.
- Vorgaben werden regelmäßig oder gar nicht eingehalten.
- Bei Sicherheitsvorfällen musste improvisiert werden und die Vorgaben wurden nicht entsprechend modifiziert.
- Wesentliche vorgegebene Dokumentationen oder Protokolle werden nicht verfasst/geführt.
- Protokolle werden nicht ausgewertet.

aber auch Erkenntnisse zur Erhöhung der Qualität bzw. allgemeinen Verbesserung:

- Die Vorgaben sind zu wenig bekannt.
- Nicht benötigte Vorgaben.
- Ungünstig formulierte Vorgaben mit hohem Schulungsaufwand.
- Bedarf für Schulung und Awareness.
- Prozesse und Abläufe, die vereinfacht oder gar eingespart werden könnten.
- Bereitstellung besserer Arbeitsmittel.

Die nächste Stufe sind Schlussfolgerungen für das Gesamtsystem, indem etwa versucht wird, Abweichungen und Trends zu finden, die sich durch mehrere Bereiche der Organisation ziehen:

- Gemeinsamkeiten bei mangelhaften Vorgaben (z. B. unverständliche Formulierung, komplizierte Beschaffung),
- Systematische Nichteinhaltungen,
- Single Points of Failure: Konzentration von Zuständigkeiten, aber auch Abweichungen an bestimmten Stellen in der Organisation,
- Schwachstellen bzw. Lücken im System.

Schließlich erfolgt die gesamtheitliche Auswertung nach:

- Vorhandensein und Qualität der Vorgaben,
- Grad ihrer Einhaltung,
- Wirkungsgrad der Maßnahmen,
- Tatsächliche (historische) oder künftige (potenzielle) Auswirkungen auf das Erreichen der Sicherheitsziele resp. Ziele der Organisation.

sowie zu:

- Empfehlungen zur Verbesserung der Vorgaben und ihrer Einhaltung,
- Empfehlungen zur Verbesserung von Prozessen und Maßnahmen.

Interner Audit Bericht

Der Bericht dient vor allem zur Dokumentation erkannter Schwachpunkte und als Checkliste für Verbesserungsmaßnahmen. Er sollte nicht redundanterweise das System, die Vorgaben oder Maßnahmen beschreiben, sondern kann davon ausgehen, das diese in der Organisation bekannt sind.

Der Bericht sollte kompakt, klar und verständlich formuliert sein und seine Gliederung für alle internen Audits möglichst gleich sein, beispielsweise wie folgt:

- Formalia (Anlass, auditierte Organisationseinheit(en), AuditorIn, Berichtsdatum, Auditzeitraum, verwendete Unterlagen, allfällige Bereiche die nicht geprüft wurden
- Management Summary der wesentlichsten Erkenntnisse aus Gesamtsicht

Jeweils pro auditierter Vorgabe:

- Bezeichnung, Inhalt
- Feststellungen (etwa: erfüllt/teilweise erfüllt/nicht erfüllt/nicht anwendbar im Einzelfall)
- Begründungen, Aussagen über die Wirksamkeit von Maßnahmen (wenn möglich)
- Empfehlungen für Maßnahmen (bei mangelhafter Erfüllung) mit Terminhorizonten bzw. allgemeine Verbesserungsvorschläge (wie Schulungsbedarf)
- Identifizierte Zuständigkeiten für die Umsetzung

sowie als Gesamtergebnis am Schluss:

- Eindruck der AuditorInnen über den Ablauf des Audits
- Zusammenfassung der wesentlichsten Erkenntnisse über alle Bereiche
- Schlussfolgerungen für das Sicherheitsniveau bzw. die Ziele der Organisation
- Zusammenfassung und Priorisierung der wichtigsten Verbesserungsvorschläge (betreffend Vorgaben wie Umsetzungen und Einhaltung)
- Zeithorizont für das nächste Audit (ggf. außerplanmäßiges Nach-Audit bei schwerwiegenden Abweichungen)

Stellungnahmen, Schlussbesprechung

Vor der offiziellen Übergabe des Auditberichts an die Managementebene sollen die betroffenen Personen bzw. Stellen Gelegenheit erhalten, zu den Erkenntnissen Stellung zu nehmen. Immerhin kann es im Zuge des Audits zu Missverständnissen oder beim Verfassen des Berichts zu Darstellungen gekommen sein, welche das Bild verzerren würden.

Eine probate Vorgehensweise besteht in der Vorab-Aussendung des Berichts oder der für die Betroffenen relevanten Teile als „Vorversion zur Stellungnahme“. Es sollte eine angemessene, aber nicht zu lange Frist für die Stellungnahmen gesetzt werden und diese sollten nach Möglichkeit schriftlich erfolgen. Es muss allen Beteiligten klar sein, dass Stellungnahmen nur berücksichtigt werden, um falsche Darstellungen im Bericht zu korrigieren, nicht aber um etwa richtigerweise erkannte Schwachstellen oder Abweichungen wegzudiskutieren. Bei größeren Meinungsverschiedenheiten kann auch ein Gespräch mit den Betroffenen sinnvoll sein. Begründete Stellungnahmen werden in die offizielle Version des Berichts eingearbeitet und diese dem Management übergeben.

An der Schlussbesprechung sollten maßgebliche MitarbeiterInnen der auditierten Organisationseinheiten sowie Mitglieder der Managementebene teilnehmen.

Die AuditorInnen präsentieren dabei das Gesamtergebnis laut Auditbericht (Ablauf des Audits, wesentliche Erkenntnisse, Schlussfolgerungen, Verbesserungsvorschläge, nächstes Audit) und sprechen allfälligen Handlungsbedarf der Managementebene an. Die betroffenen Organisationseinheiten haben die Gelegenheit für Stellungnahmen - etwa betreffend Gründe für im Audit gemachte Feststellungen.

Die Managementebene soll zum Ergebnis Stellung nehmen, erfüllte Vorgaben positiv herausstreichen aber auch seine Entschlossenheit zur Umsetzung wichtiger Verbesserungsmaßnahmen zum Ausdruck bringen. Dabei muss vor allem seitens des Managements darauf geachtet werden, dass das Ziel des Audits und der Schlussbesprechung die Optimierung von Vorgaben sowie Abläufen und des Sicherheitsniveaus ist und es sich keinesfalls um ein Tribunal handelt, bei dem MitarbeiterInnen für Nichteinhaltungen angeklagt werden.

Bei der Schlussbesprechung kann seitens des Managements bereits ein Ausblick über die Umsetzung von Verbesserungsvorschlägen samt Zeithorizont gemacht werden. Jedenfalls sollte ein Ergebnisprotokoll geführt und der Auditdokumentation beigelegt werden. Diese Dokumentation - insbesondere der Auditbericht - ist die inhaltliche Grundlage für ein nun folgendes Management-Review.

Prüfergebnisse und -berichte sind in der Regel besonders vertraulich, daher entsprechend zu schützen.

3.4 Management-Review des ISMS

> *Die Managementebene hat dafür zu sorgen, dass Maßnahmen zur Behebung von erkannten Schwachstellen, Abweichungen, Nichteinhaltung von Vorgaben etc. ergriffen werden oder aber die Ursachen beseitigt werden. Dies hat ohne unbegründete Verzögerung zu erfolgen, wenn es sich um relevante Schwachstellen handelt.*

Eine erfolgreiche Steuerung mit den dafür notwendigen Entscheidungen ist allerdings nur möglich, wenn die Managementebene einen Überblick hat, inwieweit die Sicherheitsziele mit Hilfe der eingesetzten Sicherheitsstrategie und den dafür umgesetzten Maßnahmen tatsächlich erreicht werden konnten. Weiters kann die regelmäßige Durchführung von Management-Reviews eine notwendige Voraussetzung für Akkreditierungen darstellen.

Somit muss die Managementebene das ISMS regelmäßig - zumindest einmal jährlich - überprüfen, ob es aktuell und nachhaltig zur Erreichung der Sicherheits- und Geschäftsziele geeignet und wirksam ist. Eine solche Überprüfung wird als Management-Review bezeichnet. Bei Bedarf (z. B. bei der Häufung von Sicherheitsvorfällen oder gravierenden Änderungen der Rahmenbedingungen) muss ein Management-Review auch zwischen den (jährlichen) Routineterminen abgehalten werden. Zielsetzungen des Management-Reviews sind:

- Erkennen, Abschätzen und Eliminieren von Fehlern und Schwachstellen
- Optimieren des Informationssicherheitsprozesses hinsichtlich Effizienz
- Verbesserung von Strategie, Sicherheitspolitik, -konzept, -maßnahmen, -vorgaben und Abläufen hinsichtlich Praxistauglichkeit und Einsparungspotenzial
- Optimierung von Kompetenz, Awareness der MitarbeiterInnen,
- Aufwertung der Unternehmenskultur

3.4.1 Management-Review Methoden

Sie sollen geeignet sein, einerseits den Sicherheitsprozess, andererseits die Umsetzung der Sicherheitsmaßnahmen auf ihre Angemessenheit, Wirksamkeit und Effizienz zu prüfen. Grundsätzliche Aussagen zu einer solchen Überprüfung und ihren Grundlagen sollten sich daher bereits in der Informationssicherheitsstrategie bzw. Sicherheitspolitik finden.

Wie umfassend und damit aufwändig die Grundlagen sind, hängt nicht zuletzt von der Größe und Komplexität der eigenen Organisation ab. Werden regelmäßig interne oder externe Audits durchgeführt, so sind deren Ergebnisse eine gute Grundlage für Management-Reviews. In kleinen Organisationen können ansonsten jährliche Funktionsprüfungen der IT-Systeme, Durchsicht der Dokumentation hinsichtlich Aktualität und Workshops (mit Ergebnisprotokollen) zur Diskussion von Problemen und Erfahrungen schon ausreichend sein.

Das BSI und die ISACA stellen mit dem sogenannten „Cyber-Sicherheits-Check“ [CSC] einen praxisnahen Handlungsleitfaden zur Überprüfung des aktuellen Niveaus der Cybersicherheit in einer Organisation zur Verfügung.

Wesentlich ist, dass die Managementebene ein Bild über den aktuellen Stand des Sicherheitsniveaus und allfälligen Handlungsbedarf bekommt. Beispiele für Methoden können sein:

- Berichte von internen oder externen Audits (resp. vergleichbaren Erhebungen betreffend Vorgaben und deren Erfüllung, bspw. Datenschutzkontrollen)
- Erkennen, Dokumentation, Auswertung von Sicherheitsvorfällen
- Allfällige Übungen und Tests zur Simulation von Sicherheitsvorfällen und deren Ergebnisse

- Ereignisse, Trends, Entwicklungen im Umfeld der eigenen Organisation (Gesetze, Technologien, Angriffe)
- Definition, Dokumentation und Auswertung von Kennzahlen (z.B. Aktualität des Virenschutzes und Anzahl detektierter Schadsoftware usw.)
- Zertifizierung nach festgelegten Sicherheitskriterien (z. B. ISO/IEC 27001)

Für Fragestellungen im Detail zur Erhebung und zum Erkennen von Schwachstellen und Verbesserungsmöglichkeiten siehe 3.3.2 Durchführung interner Audits.

Relevant für das Management-Review sind allerdings nicht nur aktuell erkannte Erhebungen zu Schwachstellen, sondern es müssen die - mitunter strategischen - Ursachen erforscht und Entscheidungen zur Abhilfe getroffen werden.

Für die Durchführung ist es oft zielführend einen Workshop zu veranstalten, an dem Vertreter der Managementebene, Sicherheitsbeauftragte sowie maßgebliche Führungskräfte oder Spezialisten aus den betroffenen Bereichen (etwa der IT) teilnehmen.

[Quelle: BSI-Standard 200-2]

3.4.1.1 Review der Strategie und des Sicherheitskonzepts

> *Dies ist zur kontinuierlichen Anpassung an sich laufend ändernde innere wie äußere Rahmenbedingungen notwendig. Um den Informationssicherheitsprozess erfolgreich steuern und lenken zu können, muss die Managementebene einen Überblick darüber haben, inwieweit die Sicherheitsziele mithilfe der eingesetzten Sicherheitsstrategie tatsächlich erreicht werden konnten.*

Relevante Aspekte:

- Gerade der IT-Bereich erweist sich als ausgesprochen schnelllebig. Konzepte, Maßnahmen oder Technologien, die noch vor einigen Jahren als sicher galten, können zum heutigen Zeitpunkt sicherheitstechnisch völlig überholt sein und damit gefährliche Schwachstellen darstellen, wenn man sich in trügerischer Weise darauf verlässt.
- Änderungen von relevanten Gesetzen, Vorschriften oder Normen können erheblichen Einfluss auf die Geschäftsprozesse und damit auf das Sicherheitskonzept haben.
- Änderungen innerhalb der eigenen Organisation (neue IT-Systeme, Umzug, neue Organisationsstruktur, Outsourcing) müssen schon in der Planungsphase in das Sicherheitskonzept eingearbeitet werden.

- Die Wirtschaftlichkeit der Sicherheitsstrategie und spezifischer Sicherheitsmaßnahmen - wenn auch Kosten für die Informationssicherheit schwer zu ermitteln sind - sollte regelmäßig untersucht werden: ob die tatsächlich angefallenen Kosten den ursprünglich geplanten Kosten entsprechen oder ob inzwischen ressourcenschonendere Sicherheitsmaßnahmen verfügbar sind und sinnvoll eingesetzt werden können.
- Rückmeldungen über Fehler und Schwachstellen in den Prozessen (aus Audits, aber auch Feedbacks von MitarbeiterInnen, GeschäftspartnerInnen oder KundInnen. Beschwerden von KundInnen oder MitarbeiterInnen können ein Indikator für Unzufriedenheit sein, die in der Folge eine Gefahr von fahrlässigen oder vorsätzlichen störenden Handlungen heraufbeschwören und jedenfalls die Effizienz mindern.

[Quelle: BSI-Standard 200-2]

3.4.1.2 Review der Sicherheitsmaßnahmen

> *Dies ist zur Sicherstellung der Einhaltung von Maßnahmen bei sich laufend ändernden inneren wie äußeren Rahmenbedingungen notwendig.*

Relevante Aspekte:

- Die Sinnhaftigkeit von Maßnahmen (Beitrag zum Erreichen von Sicherheitszielen) fällt in das Review der Sicherheitsstrategie
- Für ihre Umsetzung und Einhaltung ist entscheidend, ob ausreichend personelle, zeitliche und finanzielle Ressourcen zur Verfügung gestellt wurden. Der Grund für mangelhaft umgesetzte bzw. nicht eingehaltene Sicherheitsmaßnahmen können Planungsfehler oder gar unrealistische Annahmen oder Elemente der Sicherheitsstrategie bzw. des Sicherheitskonzepts sein.
- Ein weiterer Hauptgrund für nicht umgesetzte resp. nicht eingehaltene Sicherheitsmaßnahmen liegt in fehlender Akzeptanz seitens der MitarbeiterInnen. Sie kann nicht erzwungen werden, basiert aber oft im Mangel an Information, Schulung bzw. Bewusstseinsbildung.
- Wurden Vorgaben nicht eingehalten, so ist zu klären ob es an den Vorgaben (fehlend, nicht bekannt, unverständlich, unklar) oder im Bereich der für die Einhaltung Verantwortlichen liegt (Überlastung, mangelnde Motivation, Klima des Improvisierens).

[Quelle: BSI-Standard 200-2]

3.4.2 Management-Review-Ergebnis und -Auswertung

Ergebnisse sind bewertete Möglichkeiten für Änderungen resp. Verbesserungen des ISMS, der Sicherheitsstrategie, der Sicherheitspolitik und einzelner Sicherheitsmaßnahmen. Ggf. müssen, aufgrund von Veränderungen der eigenen Organisation oder des Umfelds bzw. Erfahrungen von Vorfällen, die Sicherheitsziele abgeändert werden. Jedenfalls müssen die Ergebnisse des Management-Reviews so dokumentiert werden, dass sie für die Entscheidungen und die Umsetzung von Maßnahmen geeignet sind.

Das Änderungs-/Verbesserungspotenzial kann betreffen:

- Aktualität der erkannten resp. akzeptierten Risiken
- Wirksamkeit der erkannten resp. akzeptierten Risiken
- Änderungen von Prozessen, Abläufen aufgrund des Reviews
- Verfügbarkeit von Ressourcen
- Schulungs- und Awarenessmaßnahmen, Motivationsförderung
- Aktualisierung von Dokumentationen
- Verbesserung der Methoden zur Messung der Wirksamkeit von Maßnahmen

Schließlich sind im Rahmen des Verbesserungsprozesses Entscheidungen zu treffen, ob/wann/welche Verbesserungsmaßnahmen umgesetzt werden, welche Ressourcen ihnen zugeordnet werden und unter welche Verantwortlichkeiten sie fallen.

Es kann sich herausstellen, dass die Sicherheitsziele, die Sicherheitsstrategie oder das Sicherheitskonzept geändert und die Informationssicherheitsorganisation den Erfordernissen angepasst werden sollten.

Unter Umständen ist es sinnvoll, grundlegende Änderungen an der IT-Umgebung vorzunehmen oder Geschäftsprozesse zu verändern, z. B. wenn Sicherheitsziele unter den bisherigen Rahmenbedingungen nicht oder nur umständlich (also mit hohem finanziellen oder personellen Aufwand) erreicht werden können. Wenn solche Veränderungen vorgenommen und Verbesserungen dann umgesetzt werden, schließt sich der Managementkreislauf wieder und es wird erneut mit der Planungsphase begonnen.

Die Überprüfungen zu den einzelnen Themen müssen von geeigneten Personen durchgeführt werden, die die notwendige Kompetenz und Unabhängigkeit gewährleisten können. Vollständigkeits- und Plausibilitätskontrollen sollten nicht durch die Ersteller der Konzepte vollzogen werden. Durchgeführte Verbesserungen, Korrekturen und Anpassungen sollten dokumentiert werden.

[Quelle: BSI-Standard 200-2]

3.5 Verbesserungsprozess beim ISMS

Um das angestrebte und erreichte Sicherheitsniveau dauerhaft zu gewährleisten, müssen alle für die Informationssicherheit relevanten Bereiche einem kontinuierlichen Verbesserungsprozess unterzogen werden:

- Sicherheitsstrategie, Sicherheitspolitik
- Sicherheitskonzept
- Sicherheitsmaßnahmen
- Abläufe und Verfahren
- Dokumentation
- Wissensstand und Awareness bei allen Beteiligten

Ein etablierter und dokumentierter Verbesserungsprozess ist zum einen Voraussetzung für Akkreditierung resp. Zertifizierung, zum anderen darf er nicht als administrativer Overhead gesehen werden, sondern soll alle Aktivitäten und die gesamte Organisation durchdringen. Es handelt sich dabei nicht um eine periodisch wiederkehrende Vorgangsweise, sondern vielmehr um die Summe kleinerer Schritte zur Verbesserung, die vom Management und allen MitarbeiterInnen getragen und umgesetzt werden. Vom Prinzip her ist der Verbesserungsprozess im Bereich der Informationssicherheit vergleichbar mit dem Verbesserungsprozess des Qualitätsmanagements (z. B. nach ISO 9001), der Unterschied liegt in der Sicht auf die behandelten Aspekte und Abläufe (Risikominimierung).

Der Verbesserungsprozess geschieht nicht losgelöst von den Aktivitäten, welche seine Grundlage bilden (Interne ISMS Audits sowie Management Review des ISMS), sondern umfasst vor allem die Umsetzung der dort identifizierten Verbesserungsmaßnahmen.

3.5.1 Grundlagen für Verbesserungen

Verbesserungen basieren auf Erkenntnissen aus eigenen Betriebsabläufen, Vorschlägen und externen Informationsquellen.

- Ergebnisse (Berichte, Protokolle) interner und externer Audits
- Ergebnisse (Berichte, Protokolle) des Management-Reviews
- Dokumentierte Abwicklungen von Reklamationen bzw. Beschwerden
- Vorschläge von Sicherheitsbeauftragten
- Vorschläge von MitarbeiterInnen
- Erfahrungen anderer vergleichbarer Organisationen
- Publizierte oder informelle Sicherheitswarnungen

- Informationen aus Fachpublikationen, Fachtagungen, Mitwirkung in Gremien

Ein Fokus sollte sich auf die Ursachen für erkannte Abweichungen und Gefährdungen richten. Gerade Verbesserungsvorschläge der unmittelbar befassten MitarbeiterInnen bieten ein oft unterschätztes Verbesserungs- bzw. Einsparungspotenzial, darüber hinaus wird die Motivation gestärkt wenn es zur Organisationskultur gehört, dass Mitarbeitervorschläge ernsthaft behandelt werden. Ebenso wertvoll erweisen sich gelebte Kontakte zu Sicherheitsbeauftragten anderer vergleichbarer Organisationen.

[Quelle: BSI M 2.199]

3.5.2 Entscheidungs- und Handlungsbedarf

Dieser ergibt sich für die Managementebene bei:

- Sicherheitspolitik, Sicherheitskonzept: Aktualisierung, Verbesserung, Anpassung an neue Rahmenbedingungen
- Sicherheitsmaßnahmen: Eliminieren erkannter Schwachstellen, Umstellung auf alternative Maßnahmen die effizienter sind, in der Praxis besser greifen oder weniger Ressourcen benötigen
- Implementierung: Verbesserung hinsichtlich korrekter Implementierung und Konfiguration
- Einhaltung: Organisatorische Maßnahmen, Verbesserung bei Anforderungen, Schulungen, Awareness
- Auswertung: Verbesserungen bei Protokollierung und Protokollauswertung
- Mess- und Prüfkriterien: Optimierung der Prozesse, um die Wirksamkeit und Einhaltung von Sicherheitsmaßnahmen feststellen zu können

Korrekturmaßnahmen:

Sie sollen verhindern, dass in der Praxis festgestellte Abweichungen zum Sicherheitskonzept und den Anforderungen erneut auftreten.

Für jede erkannte Abweichung sollte eine Korrekturmaßnahme vorgeschlagen und darüber entschieden werden - inklusive Zeitpunkt und Zuständigkeiten für die Umsetzung. Erkannte Fehler und Schwachstellen müssen ohne unnötigen Verzug eliminiert werden. Dabei kommen je nach Ursache in Frage:

- Anpassung organisatorischer Maßnahmen und Abläufe.
- Setzen von personellen Maßnahmen, über Schulungs- bzw. Awarenessprogramme bis hin zu disziplinären Maßnahmen oder Auswechseln von leitenden Personen.

- Planung von baulichen oder infrastrukturellen Veränderungen.
- Vornahme von technischen Veränderungen (etwa an Hard- oder Software bzw. Kommunikationseinrichtungen oder Netzwerken).

Umsetzung der Korrekturmaßnahmen:

- Alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan inkl. Terminen festhalten.
- Im Umsetzungsplan sollen Prioritäten abhängig vom jeweiligen Risiko gesetzt werden.
- Es müssen jeweils Entscheidungen der Managementebene erfolgen und dokumentiert werden - auch für den Fall, dass eine Korrekturmaßnahme verworfen wird.
- In der Folge sind jeweils die Verantwortlichen für die Umsetzung zu benennen und mit den notwendigen Ressourcen auszustatten.
- Kommunikation der umzusetzenden Maßnahmen und Verbesserungen und Abstimmung mit allen Betroffenen.
- Begleitende Kontrolle, Dokumentation und Information des Managements über Fortschritt, Fertigstellung, allfällige Abänderungen.
- Möglichst frühzeitige Prüfung der Wirksamkeit.

Vorbeugende Verbesserungsmaßnahmen:

Diese werden aufgrund der Informationslage gemäß 3.5.1 Grundlagen für Verbesserungen festgelegt, obwohl noch keine Schwachstellen wirksam geworden sind. Daher sind sie in vielen Fällen wirtschaftlicher als Korrekturmaßnahmen. Allerdings müssen zuvor nicht nur tatsächlich festgestellte, sondern auch potenzielle Schwachstellen oder Abweichungen untersucht worden sein. Dazu sind insbesondere auch Ergebnisse von:

- Geänderter Gefährdungs- oder Risikolage (aufgrund neuer Risikoanalysen, Sicherheitswarnungen, …)
- Ergebnisse von Tests
- Durchführung von Disaster Recovery-Übungen
- Übungen zur Datenrekonstruktion

heranzuziehen.

Ziel ist es, Ursachen für mögliche Abweichungen von den Anforderungen des ISMS zu eliminieren, bevor sie auftreten. Dabei ist wesentlich:

- Die zu setzenden Maßnahmen müssen in Relation zu den möglichen Auswirkungen des erkannten Problempotenzials stehen, sonst werden sie unwirtschaftlich.
- Anforderungen an Vorbeugungsmaßnahmen müssen festgelegt werden.

- Die Art der Maßnahmen entspricht weitgehend dem unter 3.5.2 Entscheidungs- und Handlungsbedarf dargestellten Entscheidungs- und Handlungsbedarf.
- Ihre Umsetzung entspricht sinngemäß der für Korrekturmaßnahmen.
- D.h. es sind Umsetzungsplan, Managemententscheidungen, benannte Verantwortliche, bereitzustellende Ressourcen sowie begleitende Kontrolle und Dokumentation notwendig.

Die laufende bzw. erfolgte Umsetzung von Konzeptänderungen oder Maßnahmen zwecks Korrektur oder Vorbeugung ist wiederum Gegenstand des ständigen Verbesserungsprozesses, womit sich der Zyklus schließt.

[Quelle: BSI M 2.199]

4 Informationssicherheitspolitik

Die Informationssicherheitspolitik bildet die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen Informationssicherheitskonzeptes. Sie stellt ein Grundlagendokument dar, das die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Methoden langfristig und verbindlich festlegt.

Die organisationsweite Informationssicherheitspolitik soll allgemeine Festlegungen treffen, die den Schutz der Informationen und der IT-Systeme innerhalb einer Organisation gewährleisten. Diese Richtlinien werden in den nachgeordneten Sicherheitsrichtlinien, etwa der E-Mail-Sicherheitsrichtlinie oder der Netzwerksicherheitsrichtlinie, konkret umgesetzt.

Ziel dieses Abschnittes ist es, die Erarbeitung einer Informationssicherheitspolitik zu unterstützen.

Das folgende Kapitel gibt eine Anleitung zur Erstellung einer derartigen Politik und legt die wesentlichen Inhalte fest. Diese sind:

- Informationssicherheitsziele und -strategien
- Erklärung der Leitungsebene über die Unterstützung der Ziele des Informationssicherheitsmanagements (Management Commitment)
- Organisation und Verantwortlichkeiten für Informationssicherheit
- Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz
- Klassifizierung von Daten
- Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity-Planung
- Aktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit
- Verweise auf weitere Dokumente zum Thema Informationssicherheit, wie etwa Sicherheitsrichtlinien

4.1 Aufgaben und Ziele einer Informationssicherheitspolitik

Eine organisationsweite Informationssicherheitspolitik hat die Aufgabe, die Vertraulichkeit, Integrität und Verfügbarkeit der Information in einer Organisation sicherzustellen.

Dabei gilt:

- Die Informationssicherheitspolitik wird als schriftliches Dokument erstellt und bildet die Grundlage des Informationssicherheitsmanagements.

- Die Informationssicherheitspolitik legt Leitlinien fest, schreibt aber keine Implementierung vor.
- Das Management unterstützt und fördert die Aktivitäten zum Informationssicherheitsmanagement. Die Informationssicherheitspolitik enthält ein explizites Statement des Managements über die Unterstützung der Informationssicherheitsziele (Management Commitment).
- Die Informationssicherheitspolitik wird offiziell verabschiedet und in Kraft gesetzt.
- Alle MitarbeiterInnen müssen Kenntnis über die wichtigsten Inhalte der Informationssicherheitspolitik haben. Die direkt mit Informationssicherheit beschäftigten MitarbeiterInnen müssen im Besitz einer aktuellen Version der Informationssicherheitspolitik sein.

Geltungsbereich

Im Bereich der öffentlichen Verwaltung ist zumindest auf Ressortebene eine eigene, ressortspezifische Informationssicherheitspolitik zu erstellen. Bei Bedarf können aus dieser weitere Informationssicherheitspolitiken, etwa auf Behörden- oder Abteilungsebene, abgeleitet werden.

Im Bereich der Privatwirtschaft wird die Erarbeitung einer organisationsweiten Informationssicherheitspolitik zumindest für große bis mittlere Unternehmen empfohlen. Abhängig von der Unternehmensstruktur und den strategischen Zielen kann die Erstellung einer Informationssicherheitspolitik auch für kleinere Unternehmen empfehlenswert sein.

4.1.1 Überprüfung und Aufrechterhaltung der Sicherheit

Informationssicherheit ist kein durch einmalige Anstrengungen erreichbarer und dann unveränderbarer Zustand. Umfassendes Informationssicherheitsmanagement beinhaltet vielmehr auch die Aufgabe, Informationssicherheit im laufenden Betrieb kontinuierlich zu überprüfen und aufrechtzuerhalten.

Die Informationssicherheitspolitik muss daher Leitlinien und Kennzahlen zur Bewertung der Sicherheit hinsichtlich Angemessenheit, Wirksamkeit und Ordnungsmäßigkeit der eingesetzten Maßnahmen sowie deren Übereinstimmung mit der Informationssicherheitspolitik und dem Informationssicherheits-Konzept vorgeben.

4.2 Inhalte der Informationssicherheitspolitik

Der folgende Abschnitt beschreibt, welche Themenbereiche im Rahmen der Informationssicherheitspolitik in jedem Fall angesprochen werden sollten, und gibt Anleitungen zur Erstellung dieses Dokumentes. Über die angeführten Themenbereiche hinaus können organisationsspezifisch weitere wichtige Sicherheitsthemen in die Informationssicherheitspolitik aufgenommen werden.

4.2.1 Informationssicherheitsziele und -strategien

Schritt 1: Festlegung der wesentlichen Informationssicherheitsziele

Im Rahmen der Erstellung der Informationssicherheitspolitik sind zunächst die spezifischen Sicherheitsziele der Organisation zu erarbeiten, die mit dieser Politik erreicht werden sollen.

Beispiele für solche Ziele sind:

- Gewährleistung der Erfüllung von aus gesetzlichen Vorgaben resultierenden Anforderungen
- Gewährleistung des Vertrauens der Öffentlichkeit in die betroffene Organisation bzw. die öffentliche Verwaltung i. Allg.
- Hohe Verlässlichkeit des Handelns, insbesondere in Bezug auf Vertraulichkeit, Richtigkeit und Rechtzeitigkeit.

Dies erfordert:

- Vertraulichkeit der verarbeiteten Informationen
- Einhaltung aller Gesetze, Verträge und Regelungen (etwa des Datenschutzgesetzes, des Informationssicherheitsgesetzes, von SLAs - Service Level Agreements - und Normen)
- Korrektheit, Vollständigkeit und Authentizität der Informationen (Integrität der IT)
- Rechtzeitigkeit (Verfügbarkeit der Daten und Services)
- Sicherung der investierten Werte
- Sicherstellung der Kontinuität der Arbeitsabläufe
- Reduzierung der im Schadensfall entstehenden Kosten (Schadensvermeidung und Schadensbegrenzung)
- Gewährleistung des besonderen Prestiges

Neben diesen eher allgemein gültigen Zielen sind die organisationsspezifischen Sicherheitsziele - bezugnehmend auf die spezifischen Aufgaben und Projekte - zu formulieren.

Zur Präzisierung dieser Ziele sind nützlicherweise folgende Fragen zu stellen:

- Welche Informationen sind besonders schützenswert?
- Welche Auswirkungen hätte eine gravierende Verletzung der Sicherheit dieser Informationen (Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit)?
- Welche wesentlichen Entscheidungen hängen von der Genauigkeit, Integrität oder Verfügbarkeit dieser Informationen ab?
- Welche essenziellen Aufgaben der betreffenden Organisation können bei Kompromittierung dieser Informationen nicht mehr durchgeführt werden?
- Welche essenziellen Aufgaben der betreffenden Organisation können ohne IT-Unterstützung nicht mehr durchgeführt werden?

Schritt 2: Festlegung des angestrebten Sicherheitsniveaus

In diesem Schritt ist festzulegen, welches Sicherheitsniveau in Bezug auf

- Vertraulichkeit
- Integrität und
- Verfügbarkeit

angestrebt werden soll.

Schritt 3: Ausarbeitung von Strategien für das Informationssicherheitsmanagement

> *Die Sicherheitsstrategie legt fest, wie die definierten Sicherheitsziele erreicht werden können.*

Eine organisationsweite Informationssicherheitspolitik kann und soll lediglich eine High-Level-Beschreibung der gewählten Strategien beinhalten, Detailbeschreibungen sind Aufgabe der nachgeordneten Sicherheitsrichtlinien.

Beispiele für Strategien für das Informationssicherheitsmanagement sind:

- eine klare Zuordnung aller Verantwortlichkeiten im Informationssicherheitsprozess
- die Einführung eines QM-Systems
- die Entwicklung von Sicherheitsrichtlinien für die wichtigsten Systeme, Services und Anwendungen
- die Etablierung eines organisationsweiten Incident Handling-Plans
- Orientierung an internationalen Richtlinien und Standards
- Informationssicherheit als integraler Bestandteil des gesamten Lebenszyklus eines IT-Systems
- die Förderung des Sicherheitsbewusstseins aller MitarbeiterInnen.

4.2.2 Management Commitment

Die Leitungsebene soll im Rahmen der Informationssicherheitspolitik ein klares Bekenntnis zur Bedeutung der Informationssicherheit für die Institution abgeben. Dazu zählen insbesondere die Unterstützung der Ziele und Prinzipien der Informationssicherheit und die Erklärung ihrer Übereinstimmung mit den Geschäftszielen und -strategien.

4.2.3 Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken

Methodisches Risikomanagement ist zur Erarbeitung eines vollständigen und organisationsweiten Informationssicherheitskonzeptes unerlässlich. Um Risiken zu beherrschen, ist es zunächst erforderlich sie zu kennen und zu bewerten. Dazu wird in einer Risikoanalyse das Gesamtrisiko ermittelt. Ziel ist es, dieses Risiko in weiterer Folge so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

In der Informationssicherheitspolitik sollen die Risikoanalysestrategie der Organisation sowie das akzeptable Restrisiko festgelegt werden. Weiters ist die Vorgehensweise bei der Akzeptanz von außergewöhnlichen Restrisiken zu definieren.

Im folgenden Abschnitt werden die wichtigsten Punkte, die im Rahmen der Informationssicherheitspolitik zum Thema Risikomanagement festgelegt werden sollten, aufgeführt. Details zur Risikoanalyse und zu Risikobehandlung sind in 5 Risikomanagement enthalten.

Schritt 1: Festlegung der anzuwendenden Risikoanalysestrategie

Man kann drei Varianten zur Risikoanalysestrategie einer Organisation unterscheiden:

- Grundschutzansatz:
  Unabhängig von den tatsächlichen Sicherheitsanforderungen werden für alle IT-Systeme Standardsicherheitsmaßnahmen („Grundschutzmaßnahmen“) eingesetzt. Diese Vorgehensweise spart Ressourcen und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzlevel für die vorhandenen Geschäftsprozesse und IT-Systeme möglicherweise nicht angemessen sein könnte.

- Detaillierte Risikoanalyse:
  Für alle Geschäftsprozesse und die sie unterstützenden IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode gewährleistet die Auswahl von effektiven und angemessenen Sicherheitsmaßnahmen, benötigt jedoch viel Zeit und Aufwand.

- Kombinierter Ansatz:

In einem ersten Schritt wird in einer Schutzbedarfsfeststellung (*High Level Risk Analysis*), ausgehend von den Geschäftsprozessen, der Schutzbedarf für die einzelnen Prozesse, die sie unterstützenden Systeme und die verarbeiteten Informationen ermittelt. Bei normalem Schutzbedarf wird von einer pauschalisierten Gefährdungslage ausgegangen, so dass auf eine detaillierte Risikoanalyse verzichtet und eine Grundschutzanalyse (s. o.) durchgeführt werden kann. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. Bei hohem Schutzbedarf können wahlweise Grundschutzmaßnahmen eingesetzt oder eine detaillierte Risikoanalyse durchgeführt werden. Besteht sehr hoher Schutzbedarf, so sind die betroffenen Geschäftsprozesse und IT-Systeme einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Die letzte Option kombiniert die Vorteile des Grundschutzansatzes mit denen einer detaillierten Risikoanalyse und stellt heute die allgemein empfohlene Vorgehensweise dar.

Schritt 2: Festlegung des akzeptablen Restrisikos

Nach Durchführung aller ausgewählten Sicherheitsmaßnahmen verbleibt i. Allg. ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. In der Informationssicherheitspolitik sind diese akzeptablen Restrisiken so exakt wie möglich zu quantifizieren und bewusst zu akzeptieren.

In der Sicherheitspolitik sollten hierzu

- generelle Richtlinien für den Prozess zur Quantifizierung und Akzeptanz von Restrisiken definiert werden, sowie
- die Risiken, die die Organisation generell bereit ist zu akzeptieren.

Schritt 3: Festlegung der Vorgehensweise zur Akzeptanz von außergewöhnlichen Restrisiken

Verbleibt im Zuge der Risikobehandlung nach Durchführung aller im Sicherheitsplan vorgesehenen Maßnahmen ein Restrisiko, das höher ist als das generell akzeptable und dessen weitere Reduktion technisch nicht möglich oder unwirtschaftlich wäre, so besteht in begründeten Ausnahmefällen die Möglichkeit einer bewussten Akzeptanz des erhöhten Restrisikos.

In der Sicherheitspolitik sind

- das Vorgehen bei Risiken, die in Abweichung von der generellen Sicherheitspolitik in Kauf genommen werden sollen, sowie
- die Verantwortlichkeiten dafür

festzulegen.

Die Entscheidung ist schriftlich zu begründen und durch die Leitung der Organisation in schriftlicher Form zu akzeptieren.

4.2.4 Dokumente zur Informationssicherheit

Abschließend sollte ein Verweis auf die wichtigsten Dokumente zum Informationssicherheitsmanagement (Sicherheitsrichtlinien, Informationen über spezielle Sicherheitsmaßnahmen oder -systeme, organisatorische Regelungen …) gegeben werden.

4.3 Lifecycle der Informationssicherheitspolitik

4.3.1 Erstellung der Informationssicherheitspolitik

Die Informationssicherheitspolitik soll von allen MitarbeiterInnen getragen werden. Es ist daher wichtig, dass bei ihrer Erstellung alle wesentlichen Kräfte der Organisation beteiligt werden und das Dokument mit VertreterInnen aller Beteiligten bzw. Betroffenen abgestimmt wird.

Zunächst ist eine verantwortliche Person für die Erstellung der Informationssicherheitspolitik zu nominieren. Im Allgemeinen wird dies, soweit bereits definiert, die/der CISO sein.

Weiters sollen VertreterInnen folgender Bereiche an der Erstellung der organisationsweiten Informationssicherheitspolitik mitarbeiten bzw. in den Abstimmungsprozess miteinbezogen werden:

- IT-Abteilung
- AnwenderInnen
- Informationssicherheitskoordinatoren im Bereich
- Personalabteilung
- Gebäudeverwaltung und Infrastruktur
- Revision
- Budgetabteilung

Die wesentlichen Inhalte der Informationssicherheitspolitik müssen allen Betroffenen und Beteiligten, also allen MitarbeiterInnen der Organisation, aber auch etwa externen MitarbeiterInnen und Lieferanten, bekannt sein.

Dazu sollten in der Folge die für die einzelnen Personengruppen wichtigsten Richtlinien und Vorgaben der Informationssicherheitspolitik zusammengefasst und allen Betroffenen in schriftlicher Form zur Kenntnis gebracht werden. Wo nötig, sind das Einverständnis mit diesen Vorgaben und die Kenntnis der daraus erwachsenden Verpflichtungen auch durch eine Unterschrift bestätigen zu lassen (etwa Verpflichtung auf das Datengeheimnis, Ergänzungen zu Dienstverträgen, Geheimhaltungsverpflichtungen von externen Personen, …).

4.3.2 Offizielle Inkraftsetzung der Informationssicherheitspolitik

Die Informationssicherheitspolitik wird von der Leitung der Organisation offiziell verabschiedet, in Kraft gesetzt und allen MitarbeiterInnen zur Verfügung gestellt.

Wesentliche Voraussetzung für eine erfolgreiche Implementierung und Umsetzung der Informationssicherheitspolitik ist, dass sie die volle und für alle Beteiligten sichtbare Unterstützung durch das Management erhält.

4.3.3 Regelmäßige Überarbeitung

Zwar stellt die Informationssicherheitspolitik ein langfristiges Dokument dar, dennoch ist auch sie regelmäßig auf ihre Aktualität und Übereinstimmung mit den tatsächlichen Anforderungen zu überprüfen und bei Bedarf entsprechend anzupassen.

Als Richtwert hierfür kann ein Zeitraum von zwei bis drei Jahren angesehen werden, nach dem die Informationssicherheitspolitik spätestens überprüft und aktualisiert werden sollte. Kommt es jedoch zwischenzeitlich zu gravierenden Änderungen im IT-System, in der Organisationsstruktur oder in den Bedrohungen, so ist eine sofortige Überarbeitung der Informationssicherheitspolitik in die Wege zu leiten.

Die Verantwortung dafür ist dezidiert festzulegen. Im Allgemeinen wird sie bei der für die IT-Sicherheit beauftragten Person liegen.

5 Risikomanagement

Wesentliches Element eines erfolgreichen Informationssicherheitsmanagements in einer Organisation ist die Etablierung und laufende Durchführung eines umfassenden Risikomanagements. Ziel des Risikomanagements ist es, relevante Risiken möglichst vollständig zu identifizieren, sowie identifizierte Risiken durch geeignete Strategien zu behandeln.

Dementsprechend gliedert sich das Risikomanagement im Wesentlichen, wie in Abbildung 5.1 dargestellt, in folgende beide Teile:

- **Risikoanalyse:** Im Rahmen der Risikoanalyse werden relevante Risiken für den definierten Geltungsbereich identifiziert. Größte Herausforderung dabei ist das Erreichen eines höchstmöglichen Grads an Vollständigkeit, sodass kein relevantes Risiko unentdeckt bleibt. Für die Durchführung einer Risikoanalyse existieren unterschiedliche Ansätze. Details zur Durchführung von Risikoanalysen im Rahmen des Risikomanagements werden im Abschnitt 5.1 näher beleuchtet. Der Fokus liegt dabei auf Risikoanalysen im Rahmen von Informationssicherheitsmanagementsystemen (ISMS), wenngleich einzelne Aspekte auch auf verwandte Themen wie architekturelle Risikoanalysen oder Risikoanalysen in den Bereichen Supply Chain Management oder Business Continuity Management anwendbar sind, die speziell auch im Rahmen der NIS2-Richtlinie von Bedeutung sind.
- **Risikobehandlung:** Im Zuge der Risikobehandlung werden die über die Risikoanalyse identifizierten Risiken adressiert und behandelt. Dafür existieren unterschiedliche Strategien. Größte Herausforderung ist es, für jedes Risiko die ideale Behandlungsstrategie zu finden. Details zur Durchführung der Risikobehandlung im Rahmen des Risikomanagements werden im Abschnitt 5.2 näher beleuchtet.

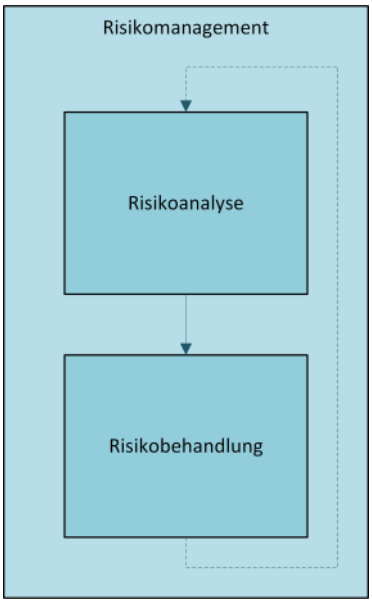

Abbildung 5.1: Wesentliche Elemente des Risikomanagements.

Das Risikomanagement versteht sich als laufender, iterativer Prozess. Nach Abschluss einer Risikobehandlung sollte daher die nächste Iteration einer Risikoanalyse anschließen, über welche die durch die zuvor durchgeführte Risikobehandlung geänderte Risikolandschaft neu bewertet wird. Die Feststellung der Wirksamkeit ausgewählter Strategien zur Behandlung identifizierter Risiken ist daher ein wesentlicher Bestandteil der Risikobehandlung selbst.

Die folgenden Abschnitte 5.1 und 5.2 geben einen Überblick über Methoden und Konzepte der Risikoanalyse und Risikobehandlung. Sie stützen sich dabei auf einschlägige Normen und Standards wie ISO/IEC 27005 oder auch die BSI-Standards 200-2 und 200-3. Die Erfahrung zeigt jedoch, dass die Umsetzung standardisierter Vorgehensweisen – insbesondere betreffend die Risikoanalyse – in der Praxis oft schwierig ist. Zumeist ist der Grund dafür der Umfang der Systeme, die über eine Risikoanalyse betrachtet werden sollen, und die damit einhergehende rasch anwachsende Komplexität der Analyse sowie ein damit verbundener schnell ausufernder Aufwand. Das vorliegende Kapitel zum Risikomanagement beschränkt sich daher nicht auf eine Zusammenfassung der wesentlichen Methoden und Konzepte zur Durchführung von Risikoanalyse und Risikobehandlung, sondern bietet in Abschnitt 5.3 außerdem praktische Handlungsempfehlungen zur Durchführung von Risikoanalysen und Risikobehandlungen.

Abgerundet wird das vorliegende Kapitel zu Risikomanagement durch die Betrachtung ausgewählter konkreter Anwendungsfälle in Abschnitt 5.4. Über diese Anwendungsfälle wird illustriert, wie Methoden und Konzepte der Risikoanalyse und Risikobehandlung in der Praxis zur Anwendung kommen. Damit bietet der Abschnitt vor allem jenen Personen, die sich neu in Themen des Risikomanagements einarbeiten wollen, einen möglichst praxisnahen und anschaulichen Einstieg.

Gegenüberstellung zu bisheriger Struktur

Das vorliegende Kapitel zu Risikomanagement wurde in der aktuellen Version des österreichischen Sicherheitshandbuchs grundlegend überarbeitet. Es ersetzt im Wesentlichen das bisherige Kapitel 4 des Sicherheitshandbuchs zu Risikoanalysen. Um Anwenderinnen und Anwendern des Sicherheitshandbuchs Orientierung zu bieten, stellt die nachfolgende Abbildung 5.2 die bisherigen und die aktuellen Inhalte dieses Kapitels gegenüber.

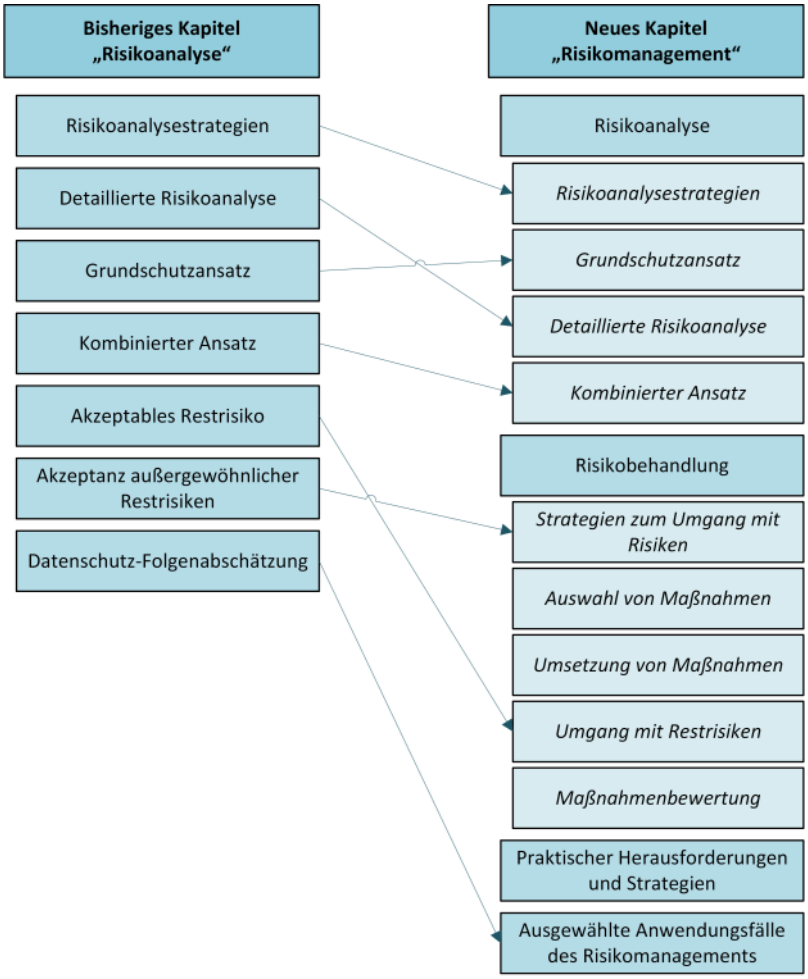

Abbildung 5.2: Gegenüberstellung der bisherigen und aktuellen Kapitelstruktur.

Abbildung 5.2 zeigt, dass das Thema Risikomanagement im aktuellen Sicherheitshandbuch breiter als bisher behandelt wird. Insbesondere erfolgt eine getrennte Betrachtung der beiden für ein erfolgreiches Risikomanagement zentralen Elemente Risikoanalyse und Risikobehandlung. Alle im bisherigen Kapitel „Risikoanalyse“ enthaltenen Elemente finden sich jedoch – in teilweise aktualisierter Form – auch in der neuen Kapitelstruktur wieder.

5.1 Risikoanalyse

Eine wesentliche Voraussetzung für erfolgreiches Informationssicherheitsmanagement innerhalb einer Organisation ist die Identifizierung und Einschätzung bestehender Sicherheitsrisiken. In einer Risikoanalyse wird versucht, diese Risiken zu erkennen und zu bewerten, um so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge im Rahmen der Risikobehandlung dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird. Die Risikoanalyse stellt damit den ersten wesentlichen Baustein eines erfolgreichen Risikomanagements dar.

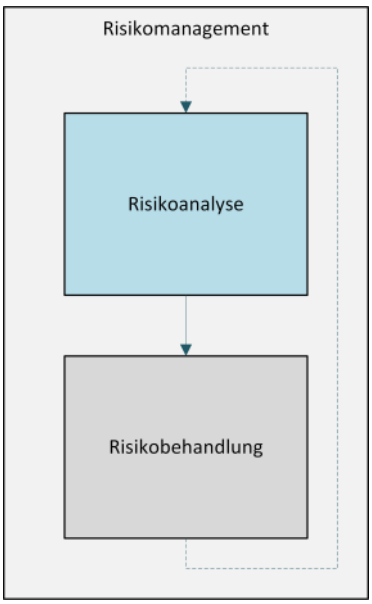

Abbildung 5.3: Rolle der Risikoanalyse im Risikomanagement.

Die Bedeutung der Risikoanalyse im Rahmen des Risikomanagements wird u.a. auch durch die NIS2-Richtlinie unterstrichen, die in Artikel 21 (2) Risikoanalysen als eine von zehn bedeutenden Risikomanagementmaßnahmen listet. Weitere Details zu Risikomanagementmethoden im Kontext der NIS2-Richtlinie finden sich auch im Abschnitt 5.4.2.

Der nachfolgende Abschnitt beschreibt drei Strategien zur Risikoanalyse - Grundschutzansatz, detaillierte Risikoanalyse und kombinierter Ansatz - und stellt ihre Vor- und Nachteile und ihre typischen Einsatzbereiche gegenüber.

5.1.1 Risikoanalysestrategien

Es ist empfehlenswert, eine Strategie zur Risikoanalyse festzulegen. Diese sollte für die gesamte Organisation gültig sein und festlegen, wie die Ziele der Risikoanalyse - Erkennen und Bewerten von Einzelrisiken und Gesamtrisiko - erreicht werden sollen.

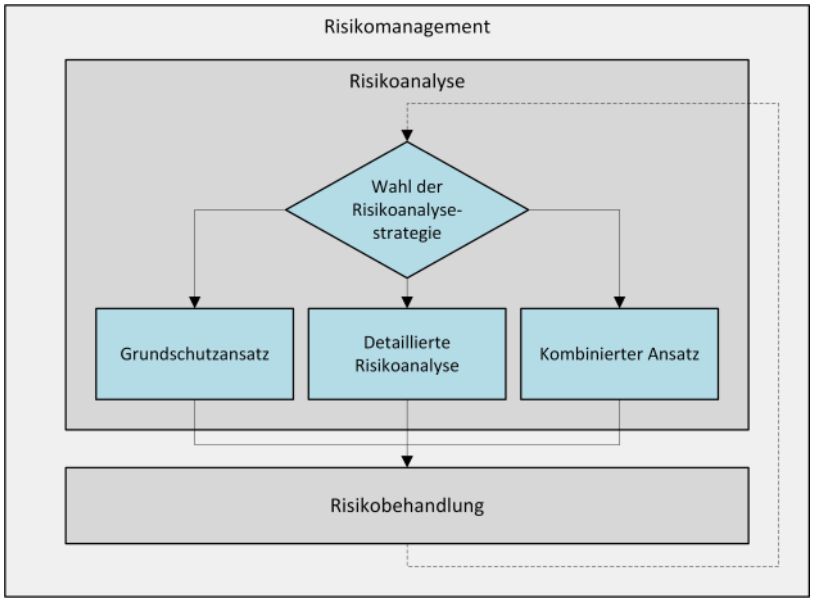

Abbildung 5.4: Risikoanalysestrategien.

Wie in Abbildung 5.4 dargestellt, kann zwischen den folgenden gängigsten Risikoanalysestrategien gewählt werden:

- **Grundschutzansatz:** Unabhängig vom tatsächlichen Schutzbedarf wird für alle relevanten IT-Systeme von einer pauschalisierten Gefährdungslage ausgegangen. Als Sicherheitsmaßnahmen kommen dann in weiterer Folge sog. Grundschutzmaßnahmen zum Einsatz. Durch den Verzicht auf eine detaillierte Risikoanalyse spart diese Vorgehensweise Ressourcen und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der Grundschutzlevel für das betrachtete IT-System möglicherweise nicht angemessen sein könnte.
- **Detaillierte Risikoanalyse:** Für die Organisation und alle ihrer relevanten IT-Systeme wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode führt zu effektiven und angemessenen Sicherheitsmaßnahmen, benötigt jedoch viel Zeit und Aufwand, sodass neben hohen Kosten auch die Gefahr besteht, dass für kritische Systeme nicht schnell genug Schutzmaßnahmen ergriffen werden können.
- **Kombinierter Ansatz:** In einem ersten Schritt wird in einer Schutzbedarfsfeststellung (*High Level Risk Analysis*) der Schutzbedarf für die relevanten IT-Systeme der Organisation ermittelt. Für IT-Systeme der Schutzbedarfskategorie „niedrig bis mittel“ wird auf eine detaillierte Risikoanalyse verzichtet und stattdessen ein Grundschutzansatz verfolgt.

Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. IT-Systeme der Schutzbedarfskategorie „hoch bis sehr hoch“ sind einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden. Der kombinierte Ansatz vereint die Vorteile des Grundschutz- und des Risikoanalyseansatzes, da alle relevanten IT-Systeme mit hohem Schutzbedarf wirksam und angemessen geschützt werden, und Maßnahmen für die anderen Systeme mit Hilfe des Grundschutzes schnell und effektiv identifiziert werden können. Der kombinierte Ansatz wird in den meisten Einsatzumgebungen die empfehlenswerte Strategie zur Risikoanalyse darstellen.

Im Folgenden werden die drei angeführten Risikoanalysestrategien näher erläutert.

5.1.2 Grundschutzansatz

Die im Rahmen dieses Handbuchs empfohlene Vorgehensweise zur Grundschutzanalyse folgt im Wesentlichen den Vorgaben zum IT-Grundschutz des BSI. In diesem Kapitel wird eine kurze Zusammenfassung des Verfahrens, angepasst an die Erfordernisse der öffentlichen Verwaltung in Österreich, gegeben.

Details zum Verfahren finden sich im BSI-Standard 200-2 sowie im IT-Grundschutz-Kompendium des BSI.

5.1.2.1 Die Idee des IT-Grundschutzes

Ziel des Grundschutzansatzes ist es, den Aufwand für die Erstellung eines an ISO/IEC 27001 angelehnten Informationssicherheitskonzeptes angemessen zu begrenzen. Dies betrifft insbesondere auch die Durchführung einer Risikoanalyse, für die der Grundschutzansatz eine im Vergleich zu einer detaillierten Risikoanalyse vereinfachte Vorgehensweise vorsieht. Der BSI-Standard 200-2 verwendet für Aspekte der Risikoanalyse, d.h. der Identifizierung relevanter Risiken, auch den Begriff „Sicherheitskonzeption“.

Die Begrenzung des mit der Risikoanalyse verbundenen Aufwands wird dadurch erreicht, dass von einer pauschalisierten Gefährdungslage ausgegangen und damit auf eine detaillierte Risikoanalyse verzichtet wird. Die Auswahl der zu realisierenden Sicherheitsmaßnahmen erfolgt auf der Basis vorgegebener Kataloge.

Die Vorteile des Grundschutzansatzes sind:

- **Geringerer Aufwand:** Der Aufwand für die Risikoanalyse wird stark reduziert.

- **Schnelle Ergebnisse:** Der Einsatz von Grundschutzmaßnahmen führt schnell zu einem hohen Niveau an Sicherheit gegen die häufigsten Bedrohungen.

Zudem sind Grundschutzmaßnahmen meist stark verbreitet und damit relativ kostengünstig und effizient zu implementieren.

Dem stehen folgende Nachteile des Grundschutzansatzes gegenüber:

- **Potenziell geringe Treffsicherheit:** Der Grundschutzlevel kann für das betrachtete System zu hoch oder zu niedrig sein. Ist er zu hoch, werden unnötige finanzielle und personelle Ressourcen verbraucht, ist er zu niedrig, bleiben unter Umständen untragbare Risiken bestehen.
- **Geringere Flexibilität:** Aufgrund der fehlenden detaillierten Risikoanalyse kann unter Umständen eine angemessene Reaktion auf sicherheitsrelevante Hard- oder Softwareänderungen schwierig sein.

Die Wahl eines Grundschutzansatzes wird daher in folgenden Fällen empfohlen:

- Wenn feststeht, dass im betrachteten Bereich nur IT-Systeme mit niedrigem oder mittlerem („normalem“) Schutzbedarf zum Einsatz kommen.
- Falls in einem Bereich (IT-System, Abteilung, …) noch keine oder offensichtlich zu schwache Sicherheitsmaßnahmen vorhanden sind, kann die Realisierung von Grundschutzmaßnahmen dazu beitragen, rasch ein relativ gutes Niveau an IT-Sicherheit zu erreichen. In diesem Fall sollte aber in einem nachfolgenden Schritt geprüft werden, ob das erreichte Niveau bereits ausreichend ist oder weitere Analysen und Maßnahmen erforderlich sind.
- Als Teil eines umfassenden Risikoanalysekonzeptes („kombinierter Ansatz“): Wird zunächst in einem ersten Schritt festgestellt, welche IT-Systeme besonders schutzbedürftig sind („Schutzbedarfsfeststellung“), so besteht die Möglichkeit, den Arbeitsaufwand für die Risikoanalyse und die Auswahl spezifischer Sicherheitsmaßnahmen auf diese hochschutzbedürftigen Systeme zu konzentrieren. Für alle anderen Systeme können Grundschutzmaßnahmen eingesetzt werden, ohne damit unangemessene Sicherheitsrisiken einzugehen. Details dazu siehe 5.1.4 Kombinierter Ansatz.

Der BSI-Standard 200-2 definiert für die Erreichung eines Grundschutzes drei verschiedene Vorgehensweisen: „Basis-Absicherung“, „Kern-Absicherung“ und „Standard-Absicherung“. Alle drei Vorgehensweisen haben zum Ziel, Risiken zu identifizieren und geeignete Sicherheitsmaßnahmen gegen diese Risiken abzuleiten. Sie unterscheiden sich jedoch in der Komplexität und damit in dem mit ihrer Durchführung verbundenen Aufwand.

Die fundamentalen Ideen hinter dem Grundschutzansatz (geringer Aufwand, schnelle Ergebnisse) werden am ehesten durch die Vorgehensweise der Basis-Absicherung erreicht. Kern- und auch Standard-Absicherung inkludieren bereits aufwändigere Elemente wie Schutzbedarfsfeststellung und Risikoanalyse. Aus diesem Grund wird für den Grundschutzansatz in diesem Abschnitt die Basis-Absicherung nach BSI-Standard 200-2 im Detail erläutert. Als Vorbereitung darauf werden nachfolgend alle drei Vorgehensweisen überblicksmäßig beschrieben.

5.1.2.2 Vorgehensweisen nach BSI-Standard 200-2

Mit „Basis-Absicherung“, „Kern-Absicherung“ und „Standard-Absicherung“ definiert der BSI-Standard für den IT-Grundschutz drei mögliche Vorgehensweisen, die sich in Bezug auf Komplexität aber auch in Bezug auf Zielgerichtetheit unterscheiden. Anwenderinnen und Anwender des IT-Grundschutz müssen sich für eine oder auch mehrere nacheinander verfolgte Vorgehensweisen entscheiden. Der BSI-Standard 200-2 empfiehlt in jedem Fall die Verfolgung der Vorgehensweise „Standard-Absicherung“, diese kann jedoch je nach Ausgangssituation über verschiedene vorangegangene Wege erreicht werden:

- Basis-Absicherung zum zügigen Erreichen eines grundsätzlichen Sicherheitsniveaus.
- Kern-Absicherung, um bei eventuell schon implementierten Maßnahmen und hoher Relevanz der Kern-Assets für die Geschäftsprozesse diese ausreichend zu schützen.
- Basis-Absicherung mit anschließender Kern-Absicherung, um bei hoher Relevanz der Kern-Assets für die Geschäftsprozesse eine schnelle Umsetzung einer Basissicherheit und einen ausreichenden Schutz der kritischen Kern-Assets zu erreichen.
- Direkte Durchführung der Standard-Absicherung ohne vorhergehender Basis- oder Kern-Absicherung.

In einzelnen Fällen ohne hohem oder sehr hohem Schutzbedarf kann auch schon eine Basis-Absicherung ausreichend sein und keine weitere Standard-Absicherung erfordern.

Basis-Absicherung

Die einfachste und damit auch am schnellsten zu Ergebnissen führende Vorgehensweise ist die Basis-Absicherung. Im Rahmen einer Basis-Absicherung sind folgende Tätigkeiten vorgesehen:

- **Festlegung des Geltungsbereichs:** Dabei wird zunächst der Anwendungsbereich (Scope) für die geplante Basis-Absicherung definiert.

- **Auswahl und Priorisierung:** Unter Verwendung vorhandener Bausteine aus dem IT-Grundschutz-Kompendium werden IT-Systeme innerhalb des definierten Anwendungsbereichs nachgebildet.
- **IT-Grundschutz-Check:** Es wird geprüft, ob Basis-Anforderungen nach dem IT-Grundschutz für die IT-Systeme im Anwendungsbereich bereits erfüllt werden oder ob sich diesbezüglich noch Lücken (Gaps) ergeben.
- **Realisierung:** Für identifizierte Gaps müssen weitere Sicherheitsmaßnahmen festgelegt und umgesetzt werden.
- **Auswahl der folgenden Vorgehensweisen:** Da die Vorgehensweise der Basis-Absicherung nur als Einstiegsvorgehensweise konzipiert ist, ist die Auswahl einer weiteren Vorgehensweise nach BSI-Standard 200-2 (Kern-Absicherung oder Standard-Absicherung) vorzunehmen und deren Umsetzung zu planen.

In Bezug auf die Betrachtung relevanter Risiken ist die Vorgehensweise der Basis-Absicherung eher rudimentär und beschränkt sich im Wesentlichen auf die Modellierung der betrachteten IT-Systeme mit Hilfe von Bausteinen aus dem IT-Grundschutz-Kompendium und auf einen einfachen Check, ob und inwieweit die mit den verwendeten Bausteinen assoziierten Sicherheitsanforderungen durch die bestehenden IT-Systeme erfüllt sind. Durch den sehr einfachen Ansatz kann diese Betrachtung in der Praxis schnell und mit wenig Aufwand vorgenommen werden.

Kern-Absicherung

Primäres Ziel der Vorgehensweise Kern-Absicherung ist es, zunächst die sogenannten Kronjuwelen einer Organisation, d.h. ihre wichtigsten Werte (Assets), zu schützen. Für diese Kronjuwelen und die mit diesen verbundenen IT-Systeme wird eine detailliertere Betrachtung relevanter Risiken vorgenommen. Dabei kommen im Wesentlichen die Methoden der Standard-Absicherung zum Einsatz. Andere, nicht geschäftskritische IT-Systeme werden hingegen vorerst nicht betrachtet.
Die Vorgehensweise der Kern-Absicherung ermöglicht es somit, besonders schützenswerte Bereiche der Organisation schnell mit einem hohen Schutzniveau abzusichern, ohne die umfangreiche und damit langwierigere Vorgehensweise hinter der Standard-Absicherung unmittelbar auf die gesamte Organisation anwenden zu müssen.

Voraussetzung für die Erstellung einer Sicherheitskonzeption über eine Kern-Absicherung ist eine Vorab-Identifizierung der Kronjuwelen der Organisation. Die Methode zur Absicherung der identifizierten Kronjuwelen über eine Betrachtung möglicher Risiken entspricht weitgehend jener der Standard-Absicherung, nur der Anwendungsbereich ist enger gefasst. Die Kern-Absicherung ist daher mit der detaillierten Risikoanalyse, die in Abschnitt 5.1.3 näher beschrieben wird, vergleichbar.

Standard-Absicherung

Während die Basis-Absicherung einen einfachen und ressourcenschonenden Einstieg in den IT-Grundschutz ermöglicht und die Kern-Absicherung sich nur auf geschäftskritische Assets konzentriert, empfiehlt das BSI in jedem Fall die Verfolgung der umfassenderen Vorgehensweise „Standard-Absicherung“. Über diese Vorgehensweise werden die zu schützenden IT-Systeme detaillierter betrachtet und notwendige Maßnahmen zu deren Absicherung zielgerichteter identifiziert. Damit einher geht allerdings auch ein höherer Aufwand in der Umsetzung dieser Vorgehensweise. Im Rahmen einer Standard-Absicherung sind folgende Tätigkeiten vorgesehen:

- **Festlegung des Geltungsbereichs:** Dabei wird zunächst der Anwendungsbereich (Scope) für die geplante Sicherheitskonzeption definiert.
- **Strukturanalyse:** Die Strukturanalyse hat zum Ziel, das Zusammenspiel von Geschäftsprozessen, Anwendungen und der zum Einsatz kommenden Informationstechnik zu analysieren und zu dokumentieren. Auf diese Weise wird über die Strukturanalyse ein Modell des relevanten Anwendungsbereichs der Organisation und ihrer IT-Systeme erstellt.
- **Schutzbedarfsfeststellung:** Über die Schutzbedarfsfeststellung wird das notwendige Schutzniveau für alle in der Strukturanalyse identifizierten und modellierten Objekte determiniert.
- **Auswahl von Anforderungen und Anpassung von Maßnahmen (Modellierung):** In diesem Schritt werden die in der Strukturanalyse identifizierten Objekte auf Bausteine des IT-Grundschutz-Kompendiums abgebildet. Auf diese Weise können allen Objekten relevante Sicherheitsanforderungen zugewiesen werden.
- **IT-Grundschutz-Check:** Es wird geprüft, ob relevante Sicherheitsanforderungen nach dem IT-Grundschutz für die IT-Systeme im Anwendungsbereich bereits erfüllt werden oder ob sich diesbezüglich noch Lücken (Gaps) ergeben.
- **Risikoanalyse:** Die Vorgehensweise der Standard-Absicherung sieht auch die Prüfung der Notwendigkeit einer zusätzlichen Risikoanalyse bei hohen oder sehr hohen Schutzbedarfen vor. Wird eine derartige Notwendigkeit erkannt, muss eine Risikoanalyse z. B. gemäß BSI-Standard 200-3 in regelmäßigen Abständen durchgeführt werden.

Im Vergleich zur Basis-Absicherung sieht die Standard-Absicherung eine detailliertere und damit auch aufwändigere Betrachtung von Risiken vor. Grundlage dafür ist eine umfassende Strukturanalyse, über die das Zusammenspiel von Geschäftsprozessen, Anwendungen und der zum Einsatz kommenden Informationstechnik analysiert und dokumentiert wird. Aufbauend darauf wird dann der Schutzbedarf der in der Strukturanalyse modellierten Objekte erhoben und Sicherheitsanforderungen dieser Objekte durch Abbildung auf das IT-Grundschutz-Kompendium identifiziert. Die Erfüllung der Sicherheitsanforderungen wird schließlich über den IT-Grundschutz-Check erhoben. Die Vorgehensweise der

Standard-Absicherung sieht auch die Prüfung der Notwendigkeit einer detaillierten Risikoanalyse vor. Insgesamt ergeben sich im Vergleich zur Basis-Absicherung bei der Standard-Absicherung damit ein deutlich höherer Aufwand, jedoch auch genauere und zielgerichtetere Ergebnisse. Die Standard-Absicherung ist damit eher mit dem Ansatz der kombinierten Risikoanalyse, die in Abschnitt 5.1.4 näher beschrieben wird, vergleichbar.

5.1.2.3 Risikoanalyse entsprechend Basis-Absicherung

Im Folgenden werden die notwendigen Schritte zur Durchführung der Risikoanalyse gemäß Grundschutzansatz erläutert. Während die grundsätzlich durchzuführenden Schritte einer Risikoanalyse im Rahmen der Basis-Absicherung oben bereits kurz skizziert wurden, werden diese in den folgenden Unterabschnitten näher beschrieben. In Abbildung 5.5 ist die Abfolge dieser Schritte dargestellt.

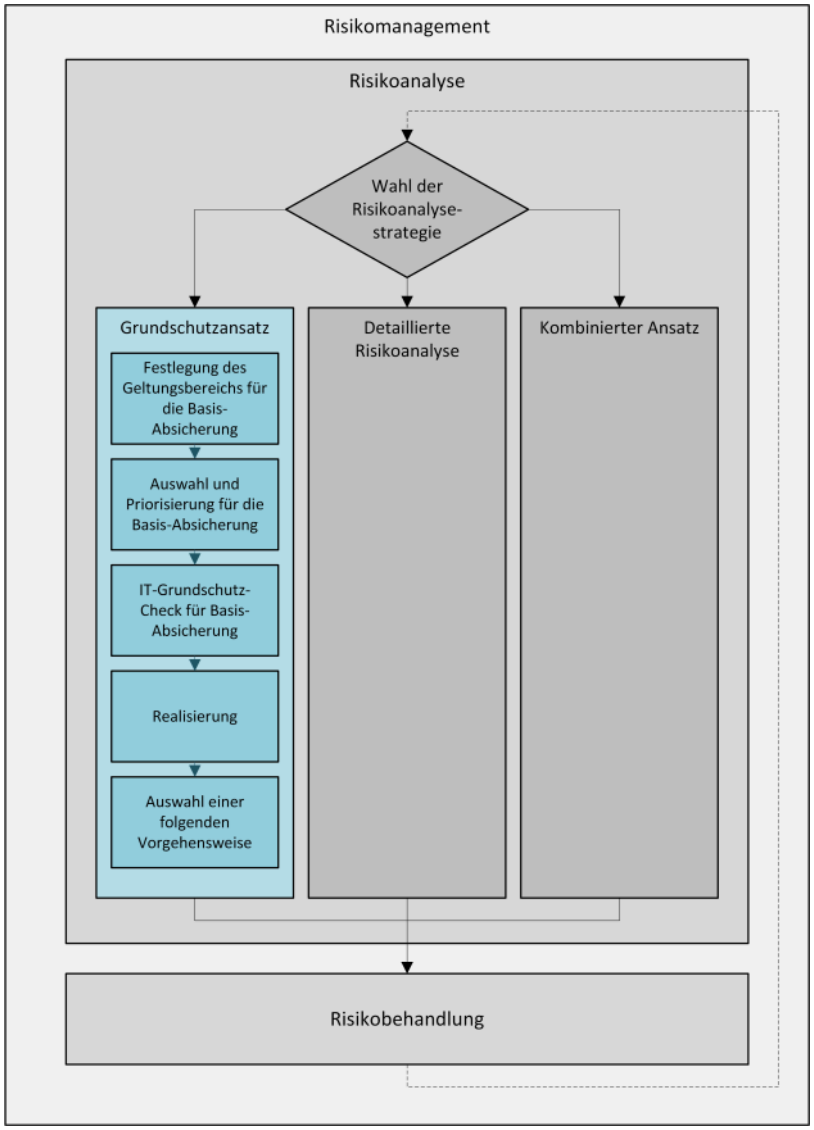

Abbildung 5.5: Wesentliche Schritte des Grundschutzansatzes.

Zu beachten ist, dass die Basis-Absicherung Konzepte der Risikoanalyse und der Risikobehandlung bewusst vermischt. Das vorliegende österreichische Sicherheitshandbuch behandelt diese Aspekte jedoch getrennt. Inhalte des Abschnitts 5.2, der sich im Detail der Risikobehandlung widmet, sollten also unbedingt mitberücksichtigt werden.

5.1.2.3.1 Festlegung des Geltungsbereichs

Der erste Schritt einer Basis-Absicherung nach BSI-Standard 200-2 besteht in der Festlegung des Geltungsbereichs (Scope-Definition). Der Geltungsbereich definiert, welche Bereiche der betreffenden Organisation von der Basis-Absicherung abgedeckt werden sollen. Dies können die gesamte Organisation oder auch klar abgrenzbare Teilbereiche davon sein.

5.1.2.3.2 Auswahl und Priorisierung

Für den definierten Geltungsbereich wird im nächsten Schritt der betrachtete Geltungsbereich innerhalb der Organisation unter Verwendung des IT-Grundschutz-Kompendiums modelliert. Dieses Modell besteht dementsprechend aus Bausteinen des IT-Grundschutz-Kompendiums, für welche unter anderem relevante Sicherheitsanforderungen definiert sind.

Aus dem erstellten Modell des Geltungsbereichs ergeben sich somit implizit alle Sicherheitsanforderungen, die für die Objekte innerhalb dieses Geltungsbereichs relevant und damit umzusetzen sind. Resultat dieses Schritts ist damit ein Prüfplan (d.h., eine Liste umzusetzender Sicherheitsanforderungen), mit dem der Geltungsbereich und die in ihm angesiedelten Objekte evaluiert werden können.

5.1.2.3.3 IT-Grundschutz-Check

Mit Hilfe des über die Modellierung des Geltungsbereichs erhaltenen Prüfplans wird im nächsten Schritt über einen Soll-Ist-Vergleich analysiert, inwieweit relevante Sicherheitsanforderungen durch Objekte im Geltungsbereich erfüllt werden. Dieser Soll-Ist-Vergleich wird als IT-Grundschutz-Check bezeichnet.

Aufgrund der bis zu diesem Schritt bereits erfolgten detaillierten Vorarbeiten ist die Durchführung des IT-Grundschutz-Checks selbst unkompliziert. Der BSI-Standard 200-2 geht trotzdem im Detail auf notwendige organisatorische Vorarbeiten und bewährte Praktiken zu dessen Durchführung ein. Als zentrales Werkzeug für die Durchführung des Soll-Ist-Vergleichs werden vorbereitete Interviews mit den jeweiligen Knowhow-Trägern nahegelegt. Zudem werden Vorgehensweisen zur Dokumentation der erhaltenen Ergebnisse empfohlen.

Gemäß BSI-Standard 200-2 sollten zu jeder Sicherheitsanforderung

- der Umsetzungsgrad (ja/teilweise/nein/entbehrlich)

sowie, soweit zu diesem Zeitpunkt bereits möglich,

- die Verantwortlichkeiten für die Umsetzung
- der Zeitpunkt für die Umsetzung und
- eine Kostenschätzung

angegeben werden. Zudem sollen getroffene Entscheidungen bezüglich des Umgangs mit nicht oder nur teilweise erfüllten Anforderungen dokumentiert werden, um sie auch noch zu späteren Zeitpunkten nachvollziehen zu können. Details zum Umgang mit identifizierten Mängeln und damit verbundenen Risiken sind in 5.2 Risikobehandlung angeführt.

5.1.2.3.4 Realisierung

Nach Durchführung des IT-Grundschutz-Checks sieht der BSI-Standard 200-2 als nächstes den Schritt der Realisierung vor, in dem aus den Resultaten des IT-Grundschutz-Checks konkrete umzusetzende Sicherheitsmaßnahmen abgeleitet werden.

Dies umfasst die Tätigkeiten „Sichtung der Untersuchungsergebnisse“, „Konsolidierung der Basis-Anforderungen“, „Kosten- und Aufwandsschätzung“, „Festlegung der Umsetzungsreihenfolge der Basis-Anforderungen“, „Festlegung der Aufgaben und Verantwortung“, und „Realisierungsbegleitende Basis-Anforderungen“. Die mit diesem Schritt („Realisierung“) in Verbindung stehenden Tätigkeiten betreffen damit den Bereich Risikobehandlung, dessen relevante Aspekte im Abschnitt 5.2 näher diskutiert werden.

5.1.2.3.5 Auswahl einer folgenden Vorgehensweise

Abschließend weist der BSI-Standard 200-2 darauf hin, dass eine Basis-Absicherung stets nur ein erster Schritt, das mittelfristige Ziel aber immer eine Kern- bzw. Standard-Absicherung sein sollte. Dies entspricht sinngemäß den Risikoanalysestrategien „Detaillierte Risikoanalyse“ bzw. „Kombinierter Ansatz“ des österreichischen Sicherheitshandbuchs. Diese Strategien werden jeweils in den Abschnitten 5.1.3 und 5.1.4 näher beschrieben.

5.1.3 Detaillierte Risikoanalyse

Eine detaillierte Risikoanalyse für eine Organisation oder ein IT-System umfasst die Identifikation der bestehenden Risiken sowie eine Abschätzung der Größe dieser Risiken. Dazu werden im Wesentlichen relevante Werte (Assets), Bedrohungen und Schwachstellen identifiziert und die daraus resultierenden Risiken ermittelt.

Die Durchführung einer detaillierten Risikoanalyse ist in der Regel umfangreich. Dies liegt an der einer detaillierten Risikoanalyse inhärenten Systematik, die zur Sicherstellung einer möglichst vollständigen Betrachtung notwendig ist. Zudem sollte eine detaillierte Risikoanalyse einen geeigneten Detailgrad erreichen, damit ihre Resultate aussagekräftig sind. Die erstmalige Durchführung einer detaillierten Risikoanalyse und die anschließende Erstellung eines Sicherheitskonzeptes erfordern daher in der Regel einen Aufwand, der zumindest im Bereich von Wochen, möglicherweise auch von Monaten liegt.

Es existieren diverse Normen und Standards, die Methoden zur Durchführung detaillierter Risikoanalysen beschreiben. Beispiele sind der BSI-Standard 200-3 oder auch ISO/IEC 27005. Auch wenn sich einschlägige Normen und Standards in Details unterscheiden, so ähneln sich die meisten von ihnen doch in Bezug auf den grundsätzlichen Ansatz zur Durchführung von Risikoanalysen. Dieser grundlegende Ansatz und seine einzelnen Analyseschritte werden im folgenden Abschnitt zunächst überblicksmäßig beschrieben und in weiterer Folge im Detail erklärt.

Vergleich zu anderen Risikoanalysestrategien

Eine detaillierte Risikoanalyse ist damit weit aufwändiger als eine Risikoanalyse nach dem oben beschriebenen Grundschutzansatz. Allerdings kann davon ausgegangen werden, dass auch die Resultate einer detaillierten Risikoanalyse (welche Risiken existieren, welche Komponenten und Systeme betreffen sie und wie hoch sind die Risiken) entsprechend genauer und zielgerichteter sind.

Die größte Herausforderung in der Durchführung detaillierter Risikoanalysen ist der Umgang mit der damit verbundenen Komplexität und die Vermeidung eines zu hohen Aufwands. Die im nächsten Abschnitt beschriebene Risikoanalysestrategie des kombinierten Ansatzes kann hier Abhilfe schaffen.

5.1.3.1 Analyseschritte

Die Durchführung einer detaillierten Risikoanalyse gliedert sich in mehrere Schritte. Abhängig vom zugrundeliegenden Standard (BSI-Standard 200-3, ISO/IEC 27005, etc.) sind diese Schritte leicht unterschiedlich ausgeformt. Im Wesentlichen folgen sie aber stets einer ähnlichen grundlegenden Methodik. In der Folge sind übliche Schritte einer detaillierten Risikoanalyse in der vorgesehenen Reihenfolge ihrer Durchführung überblicksmäßig beschrieben.

Bei der Durchführung einer Risikoanalyse über die unten angeführten Schritte sind folgende allgemeine Prinzipien zu beachten:

- Das gesamte Verfahren muss transparent gemacht werden.
- Es dürfen keine versteckten Annahmen gemacht werden, die z. B. dazu führen, dass Bedrohungen nicht betrachtet werden.
- Alle Bewertungen müssen begründet werden, um subjektive Einflüsse zu erkennen und so weit wie möglich zu vermeiden.
- Alle Schritte müssen so dokumentiert werden, dass sie später auch für andere nachvollziehbar sind. Ein derartiges Vorgehen erleichtert auch eine spätere Überarbeitung des Informationssicherheitskonzeptes.
- Der Aufwand für die Durchführung des Verfahrens sollte dem Wert der IT-Anwendungen und den Werten der Organisation i. Allg. angemessen sein.

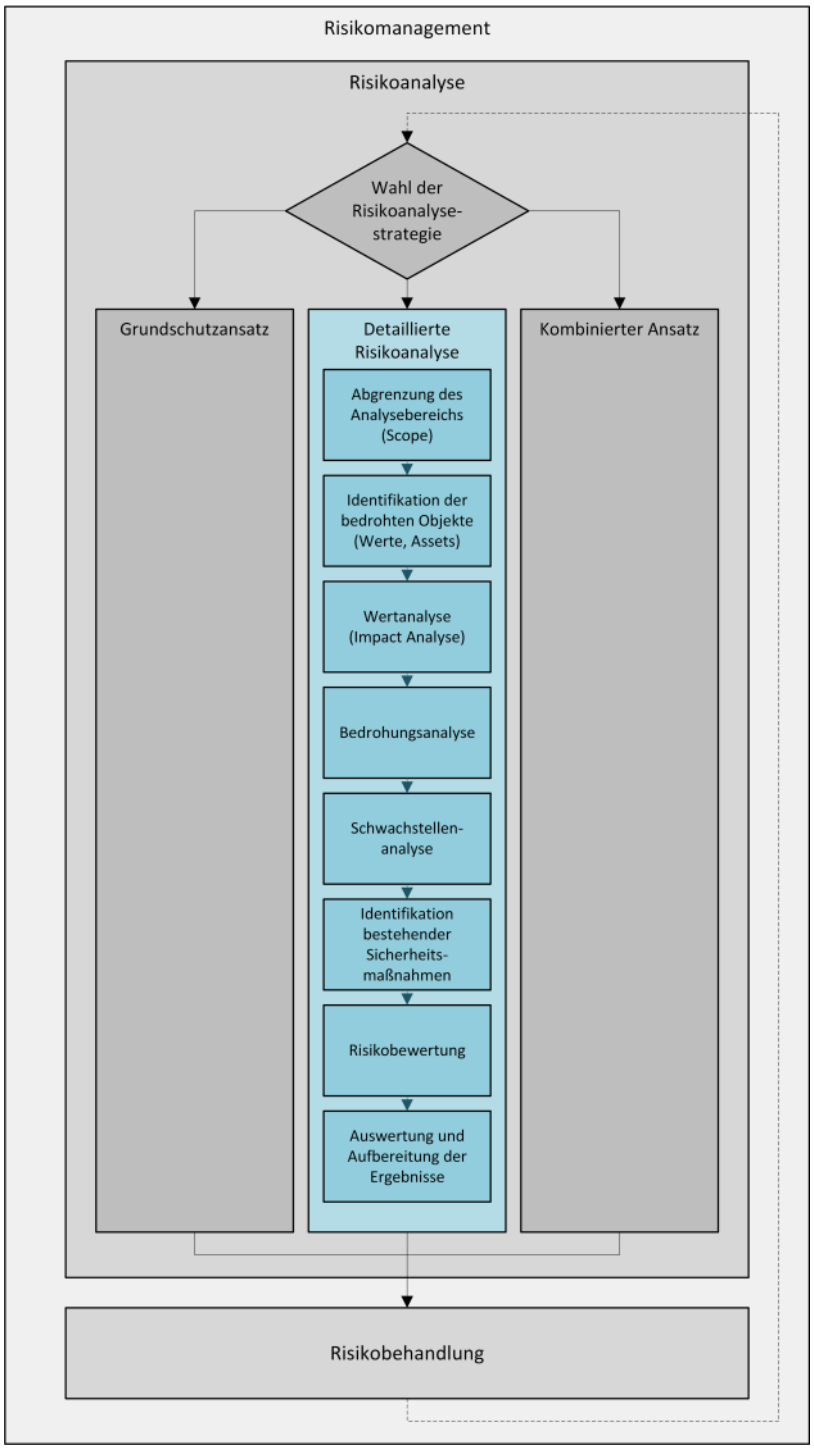

Abbildung 5.6: Wesentliche Schritte der detaillierten Risikoanalyse.

Unter Berücksichtigung dieser Prinzipien gliedert sich die Durchführung einer detaillierten Risikoanalyse in folgende, auch in Abbildung 5.6 dargestellte, Schritte:

Schritt 1: Abgrenzung des Analysebereiches (Scope)

Hier sind die zu analysierenden Organisationsteile bzw. ihre IT-Systeme zu spezifizieren und anzugeben, ob und in welchem Maße auch andere Objekte (z. B. Gebäude und Infrastruktur) in die Analyse einbezogen werden sollen.

Schritt 2: Identifikation der bedrohten Objekte (Werte, Assets)

Ziel dieses Schrittes ist die Erfassung aller bedrohten Objekte, die innerhalb des im vorangegangenen Schritt festgesetzten Analysebereiches liegen.

Schritt 3: Wertanalyse (Impact Analyse)

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt.

Die Wertanalyse umfasst im Einzelnen:

- die Festlegung der Bewertungsbasis für Sachwerte
- die Festlegung der Bewertungsbasis für immaterielle Werte
- die Ermittlung der Abhängigkeiten zwischen den Objekten
- die Bewertung der bedrohten Objekte und der möglichen Schäden (Impact Analyse)

Schritt 4: Bedrohungsanalyse

Die ermittelten Objekte sind vielfachen Bedrohungen ausgesetzt, die sowohl aus Nachlässigkeit und Versehen als auch aus Absicht resultieren können.

Die Bedrohungsanalyse umfasst:

- die Identifikation möglicher Bedrohungen (Katastrophen, Fehlbedienung, bewusste Angriffe, etc.) und möglicher AngreiferInnen (MitarbeiterInnen, Leasingpersonal, Außenstehende, etc.)
- die Ermittlung der Eintrittswahrscheinlichkeiten

Schritt 5: Schwachstellenanalyse

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Es ist daher erforderlich, mögliche Schwachstellen der analysierten Organisation bzw. des analysierten Systems zu identifizieren und ihre Bedeutung zu klassifizieren.

Zu untersuchen sind dabei insbesondere die Bereiche Organisation, Hard- und Software, Personal sowie Infrastruktur.

Schritt 6: Identifikation bestehender Sicherheitsmaßnahmen

Zur Vermeidung unnötiger Aufwände und Kosten sind die bereits existierenden Sicherheitsmaßnahmen zu erfassen und auf ihre Auswirkungen hinsichtlich der Gesamtsystemsicherheit sowie auf korrekte Funktion zu prüfen.

Geplante neue Sicherheitsmaßnahmen müssen mit den existierenden Maßnahmen kompatibel sein und eine wirtschaftlich und technisch sinnvolle Ergänzung darstellen.

Schritt 7: Risikobewertung

In diesem Schritt werden die Einzelrisiken und das Gesamtrisiko ermittelt und bewertet.

Schritt 8: Auswertung und Aufbereitung der Ergebnisse

Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse ab.

Die einzelnen oben identifizierten Schritte einer detaillierten Risikoanalyse werden in den folgenden Unterabschnitten ausführlicher behandelt. Das vorliegende Handbuch gibt Hinweise und Unterstützung zur Durchführung dieser Schritte. Weitere praktische Aspekte der Durchführung von Risikoanalysen werden auch in 5.3 Praktische Herausforderungen und Strategien diskutiert.

Die Wahl einer konkreten Methode für die Durchführung der einzelnen Schritte sowie ein etwaiger Einsatz von Tools zur Unterstützung dieser Analyse bleiben der durchführenden Organisation überlassen. Wichtig ist jedoch, dass alle der im Folgenden angeführten Schritte durchlaufen werden und die geforderten Ergebnisse liefern.

5.1.3.1.1 Abgrenzung des Analysebereiches (Scope)

Vor Beginn einer Risikoanalyse ist es erforderlich, den zu analysierenden Bereich genau abzugrenzen. Das betrifft einerseits den relevanten Bereich der zu analysierenden Organisation und andererseits auch die relevanten Komponenten der IT-Systeme der Organisation. In Bezug auf die Organisation kann der Analysebereich z.B. auf bestimmte Teile der Organisationsstruktur (Standorte, Geschäftsbereiche, etc.) eingeschränkt werden. Abhängig davon kann auch eine Einschränkung der betrachteten Komponenten der IT-Systeme der Organisation erfolgen.

In jedem Fall ist im Zuge der Abgrenzung auch anzugeben, ob sich die Analyse auf Hardware, Software und Daten der betrachteten Organisation beschränkt, oder ob und in welchem Ausmaß andere Werte wie Gebäude und Infrastruktur, Personen, immaterielle Güter, Fähigkeiten und Leistungen ebenfalls einbezogen werden sollen.

Ergebnis der Abgrenzung des Analysebereichs (Scope):

Definierter Scope der Risikoanalyse.

5.1.3.1.2 Identifikation der bedrohten Objekte (Werte, Assets)

In diesem Schritt sind alle bedrohten Objekte (Assets), die innerhalb des festgestellten Analysebereiches liegen, zu erfassen.

Unter den bedrohten Objekten einer Organisation ist alles zu verstehen, was für diese schutzbedürftig ist, also alle Objekte, von denen der Betrieb der IT-Systeme und ihre Anwendungen und damit die Funktionsfähigkeit der Organisation abhängen. Dazu zählen etwa:

- **Physische Objekte:** Beispielsweise Gebäude, Infrastruktur, Hardware, Datenträger, Dokumente.
- **Logische Objekte:** Beispielsweise Software, Daten, Information.
- **Personen:** MitarbeiterInnen, etc.
- **Fähigkeiten:** Etwa Herstellen eines Produktes oder Erbringen einer Dienstleistung.
- **Immaterielle Güter:** Beispielsweise Image, Vertrauen in die Organisation oder gute Beziehungen zu anderen Organisationen und Institutionen.

Zwischen den bedrohten Objekten bestehen grundsätzlich komplexe Abhängigkeiten. Die Vertraulichkeit, Integrität oder Verfügbarkeit eines Objektes setzt vielfach die Vertraulichkeit, Integrität oder Verfügbarkeit eines anderen Objektes voraus. Beispiele dafür sind etwa das Erfordernis einer funktionsfähigen Infrastruktur (Stromversorgung, Klimaanlage, etc.) für den Betrieb eines IT-Systems oder die Abhängigkeit der Software von unversehrter und verfügbarer Hardware.

Die Identifizierung der bedrohten Objekte sowie ihre nachfolgende Bewertung stellen wesentliche Voraussetzungen für ein erfolgreiches Informationssicherheitsmanagement dar. Dabei ist es den Erfordernissen im Einzelfall anzupassen, in welcher Tiefe und in welchem Detaillierungsgrad die einzelnen Objekte analysiert werden sollen; in vielen Fällen wird eine Zusammenfassung in Gruppen sinnvoll sein und dazu beitragen, den Analyseaufwand zu begrenzen.

Ergebnis der Identifikation der bedrohten Objekte (Werte, Assets):

Aufstellung der im Analysebereich (Scope) befindlichen bedrohten Objekte der Organisation.

5.1.3.1.3 Wertanalyse (Impact Analyse)

In diesem Schritt wird der Wert der im vorangegangenen Schritt identifizierten Objekte ermittelt.

Die Wertanalyse umfasst im Einzelnen die folgenden Schritte, die nachfolgend noch näher beschrieben werden:

- Festlegung der Bewertungsbasis für Sachwerte
- Festlegung der Bewertungsbasis für immaterielle Werte
- Ermittlung der Abhängigkeiten zwischen den Objekten
- Bewertung der bedrohten Objekte und der möglichen Schäden

Ergebnis der Wertanalyse:

Aufstellung der relevanten bedrohten Objekte der Organisation und ihrer Werte.

Schritt 1: Festlegung der Bewertungsbasis für Sachwerte

Zunächst ist zu entscheiden, ob die Bewertung quantitativ oder qualitativ erfolgen soll. In der Regel wird eine quantitative Bewertung präferiert, da eine solche exaktere Einstufungen erlaubt. Nicht immer ist jedoch eine quantitative Bewertung möglich.

Eine quantitative Bewertung kann etwa beruhen auf

- dem Zeitwert eines Objektes,
- dem Wiederbeschaffungswert eines Objektes,
- dem Wert, den das Objekt für potenzielle AngreiferInnen hätte, oder
- dem Schaden, der sich aus dem Verlust oder der Modifikation eines zu schützenden Objektes für die betroffene Organisation ergibt.

Eine qualitative Bewertung erfolgt durch Einteilung in Klassen. Beispiele hierfür sind etwa:

- **3-stufige Bewertung:** gering - mittel - hoch
- **5-stufige Bewertung:** unbedeutend - gering - mittel - hoch - sehr hoch

Als Basis für eine qualitative Bewertung ist festzulegen, was die einzelnen Klassen bedeuten bzw. wie sie definiert sind.

Schritt 2: Festlegung der Bewertungsbasis für immaterielle Werte

Auch für immaterielle Werte, wie etwa Bewahrung des guten Rufes oder Gewährleistung der Vertraulichkeit, kann eine quantitative oder eine qualitative Bewertungsbasis festgelegt werden.

Eine quantitative Bewertung kann in diesem Fall beruhen auf

- dem Wert, den das Objekt für einen potenziellen Angreifer hätte (z. B. vertrauliche Information), oder
- dem Schaden, der sich aus einem Angriff auf das zu schützende Objekt für die betroffene Organisation ergibt.

Es ist zu beachten, dass die potenziellen Schäden den eigentlichen (Zeit- oder Wiederbeschaffungs-)Wert beträchtlich übersteigen können.

Schritt 3: Ermittlung der Abhängigkeiten zwischen den Objekten

Es ist wichtig, auch gegenseitige Abhängigkeiten von Objekten festzustellen, da diese Abhängigkeiten Einfluss auf die Bewertung der einzelnen zu schützenden Objekte haben kann.

So ist etwa die Funktionsfähigkeit von Hardware abhängig von der Funktionsfähigkeit der Stromversorgung und eventuell der Klimaanlage. Die Integrität von Information bedingt die Integrität und Verfügbarkeit der Hard- und Software, die zu ihrer Verarbeitung bzw. Speicherung eingesetzt wird.

Die Ermittlung und Modellierung von Abhängigkeiten zwischen Objekten ist in der Praxis ein komplexes und damit aufwändiges Unterfangen, für die Aussagekraft der Risikoanalyse jedoch sehr relevant.

Schritt 4: Bewertung der bedrohten Objekte und der möglichen Schäden

Mit Ausnahme der Festsetzung von Zeit- oder Wiederbeschaffungswert wird die Bewertung von bedrohten Objekten in der Regel sehr subjektiv sein. Es ist daher notwendig, im Rahmen der Analyse möglichst genaue Bewertungsbasen und Regeln vorzugeben und diese eventuell durch Beispiele zu illustrieren sowie möglichst viele unterschiedliche Personen nach ihrer Einschätzung zu befragen.

Durchführung:

- Die Person, die die Risikoanalyse durchführt, erstellt eine Liste der zu bewertenden Objekte und gibt die Bewertungsbasen vor.
- Die Bewertung sollte durch die Applikations-/Projektverantwortlichen sowie die betroffenen BenutzerInnen vorgenommen werden.

- Unterstützung in der Bewertung kann von verschiedenen Abteilungen, etwa Finanzen, Einkauf, IT, etc. kommen.
- Es ist Aufgabe derjenigen Person, die die Risikoanalyse durchführt, die einzelnen Bewertungen auf Plausibilität und Konsistenz zu prüfen und ein konsolidiertes Ergebnis zu erarbeiten.

5.1.3.1.4 Bedrohungsanalyse

Laut [ISO/IEC 27000] ist eine Bedrohung eine „mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation führen kann“.

Die zu schützenden Objekte sind vielfältigen Bedrohungen ausgesetzt. Im Rahmen der Risikoanalyse müssen diese Bedrohungen möglichst vollständig identifiziert werden, weiters ist ihre Schwere und Eintrittswahrscheinlichkeit abzuschätzen.

Bedrohungen sind charakterisiert durch:

- ihren Ursprung:
  Bedrohungen durch die Umwelt oder durch den Menschen, wobei letztere wieder in absichtliche oder zufällige Bedrohungen zu unterteilen sind. Im Falle absichtlicher Bedrohungen ist zwischen Innen- und Außentäter zu unterscheiden.
- die Motivation:
  Motivation für (absichtliche) Bedrohungen können etwa finanzielle Gründe, Wettbewerbsvorteile, Rache, aber auch Geltungssucht oder erhoffte Publicity sein.
- die Häufigkeit des Auftretens,
- die Größe des Schadens, der durch diese Bedrohung verursacht werden kann.

Für einige umweltbedingte Bedrohungen (etwa Erdbeben, Blitzschlag, Hochwasser, …) liegen statistische Daten vor, die für die Einschätzung hilfreich sein können.

Die Bedrohungsanalyse umfasst im Einzelnen die folgenden Schritte, auf die unten noch im Detail eingegangen wird:

- Identifikation möglicher Bedrohungen
- Ermittlung der Eintrittswahrscheinlichkeiten

Ergebnis der Bedrohungsanalyse:

Liste von Bedrohungen, der von ihnen bedrohten Objekte, und ihrer Eintrittswahrscheinlichkeiten.

Schritt 1: Identifikation möglicher Bedrohungen

Bedrohungen werden nach Kategorien unterteilt:

- Höhere Gewalt
  (etwa Blitzschlag, Feuer, Hochwasser, Erdbeben, Personalausfall)
- Organisatorische Mängel
  (etwa fehlende oder unzureichende Regelungen für Wartung, Dokumentation, Test und Freigabe, fehlende Auswertung von Protokolldaten, mangelhafte Kennzeichnung von Datenträgern)
- Menschliche Fehlhandlungen
  (etwa fehlerhafte Systemnutzung oder -administration, fahrlässige Zerstörung von Geräten oder Daten, Nichtbeachtung von Sicherheitsmaßnahmen)
- Technisches Versagen
  (etwa Ausfall von Versorgungs- und Sicherheitseinrichtungen, Softwarefehler, defekte Datenträger)
- Vorsätzliche Handlungen
  (etwa Manipulation/Zerstörung von Geräten, Manipulation an Daten oder Software, Viren, trojanische Pferde, Abhören, Wiedereinspielen von Nachrichten, Nichtanerkennen einer Nachricht, Maskerade)

Es ist wichtig, alle wesentlichen Bedrohungen möglichst vollständig zu erfassen, da andernfalls Sicherheitslücken bestehen bleiben können.

Bei der Identifikation von möglichen Bedrohungen können Bedrohungskataloge hilfreich sein, die den Charakter von Checklisten haben. Solche Kataloge finden sich etwa in [BSI 7105] und in [ISO/IEC 27005]. Im IT-Grundschutz-Kompendium des BSI gibt es eine umfangreiche Sammlung von so genannten „Gefährdungen“, die ihrerseits eine Kombination aus Bedrohungen und Schwachstellen darstellen. Es ist jedoch zu betonen, dass keine derartige Liste vollständig sein kann, und darüber hinaus auch Bedrohungen einem ständigen Wandel und einer ständigen Weiterentwicklung unterworfen sind. Es ist daher immer erforderlich, über Bedrohungskataloge hinaus auch die Möglichkeit weiterer Bedrohungen in Betracht zu ziehen.

Schritt 2: Bewertung möglicher Bedrohungen

In diesem Schritt der Risikoanalyse ist zu bestimmen, mit welcher Wahrscheinlichkeit eine Bedrohung im betrachteten Umfeld eintreten wird.

Diese ist abhängig von:

- der Häufigkeit der Bedrohung (Wahrscheinlichkeit des Auftretens anhand von Erfahrungen, Statistiken, …),
- der Motivation und den vorausgesetzten Fähigkeiten und Ressourcen potenzieller AngreiferInnen,

- Einschätzung der Attraktivität und Verwundbarkeit des IT-Systems bzw. seiner Komponenten,
- Umweltfaktoren und organisationsspezifischen Einflüssen.

Auch die Eintrittswahrscheinlichkeit kann quantitativ oder qualitativ bewertet werden.

Da eine quantitative Bewertung in vielen Fällen eine Genauigkeit vortäuschen könnte, die durch die ungenaue Methode der Schätzung nicht zu rechtfertigen ist, ist in den letzten Jahren ein Trend in Richtung qualitativer Bewertung zu erkennen.

Bewährt haben sich hier etwa drei- bis fünfteilige Skalen, wie beispielsweise:

- 4: sehr häufig
- 3: häufig
- 2: mittel
- 1: selten
- 0: sehr selten

Diese allgemeinen Bedeutungen der Skalenwerte sind für den spezifischen Anwendungsbereich zu konkretisieren, zum Beispiel:

- 4: einmal pro Minute
- 3: einmal pro Stunde
- 2: einmal pro Tag
- 1: einmal pro Monat
- 0: einmal im Jahr

5.1.3.1.5 Schwachstellenanalyse

Unter einer Schwachstelle (Vulnerability) versteht man eine Sicherheitsschwäche eines oder mehrerer Objekte, die durch eine Bedrohung ausgenützt werden kann.

Typische Beispiele für Schwachstellen sind etwa:

- Mangelnder baulicher Schutz von Räumen mit IT-Einrichtungen
- Nachlässige Handhabung von Zutrittskontrollen
- Spannungs- oder Temperaturschwankungen bei Hardwarekomponenten
- kompromittierende Abstrahlung
- Spezifikations- und Implementierungsfehler
- schwache Passwortmechanismen
- unzureichende Ausbildung, mangelndes Sicherheitsbewusstsein

Eine Schwachstelle selbst verursacht noch keinen Schaden, sie ist aber die Voraussetzung, die es einer Bedrohung ermöglicht, wirksam zu werden und damit ein IT-System zu beeinträchtigen. Auf Schwachstellen, für die eine korrespondierende Bedrohung existiert, sollte daher sofort reagiert werden.

Eine *Schwachstellenanalyse* ist die Überprüfung von Sicherheitsschwächen, die durch festgestellte Bedrohungen ausgenutzt werden können. Diese Analyse muss sowohl das Umfeld als auch bereits vorhandene Schutzmaßnahmen mit einbeziehen. Es ist wichtig, jede Schwachstelle daraufhin zu bewerten, wie leicht es ist, sie auszunutzen

Beispielhafte Auflistungen von Schwachstellen, die auf typische Problembereiche hinweisen, finden sich etwa in [ISO/IEC 27005] Annex D sowie in [BSI 7105].

Ergebnis der Schwachstellenanalyse:

Liste von potenziellen Schwachstellen mit Angaben darüber, wie leicht diese für einen Angriff ausgenützt werden können.

5.1.3.1.6 Identifikation bestehender Sicherheitsmaßnahmen

Sicherheitsmaßnahmen sind Verfahrensweisen, Prozeduren und Mechanismen, die eine oder mehrere der nachfolgenden Funktionen erfüllen:

- Vermeidung von Risiken,
- Verkleinerung von Bedrohungen oder Schwachstellen,
- Entdeckung unerwünschter Ereignisse,
- Eingrenzung der Auswirkungen eines unerwünschten Ereignisses,
- Überwälzung von Risiken oder
- Wiederherstellung eines früheren Zustandes.

Wirksame IT-Sicherheit verlangt i. Allg. eine Kombination von verschiedenen Typen von Maßnahmen.

Da die Sicherheitsmaßnahmen, die im Rahmen der Risikobehandlung (siehe Abschnitt 5.2) aufgrund einer Risikoanalyse ausgewählt werden, in der Regel zusätzlich zu bereits bestehenden Maßnahmen eingeführt werden sollen, ist es notwendig, alle bereits existierenden oder geplanten Sicherheitsmaßnahmen zu identifizieren und ihre Auswirkungen zu überprüfen, um unnötigen Aufwand zu vermeiden.

Stellt sich heraus, dass eine bereits existierende oder geplante Maßnahme ihren Anforderungen nicht gerecht wird, so ist zu prüfen, ob sie ersatzlos entfernt, durch andere Maßnahmen ersetzt bzw. ergänzt oder aus Kostengründen belassen werden soll.

Im Rahmen dieses Schrittes sollte auch geprüft werden, ob die bereits existierenden Sicherheitsmaßnahmen korrekt zum Einsatz kommen. Falsch oder unvollständig eingesetzte Sicherheitsmaßnahmen stellen eine zusätzliche potenzielle Schwachstelle eines Systems dar.

Ergebnis der Ist-Stand-Erhebung:

Aufstellung aller bereits existierenden oder geplanten Sicherheitsmaßnahmen mit Angaben über ihren Implementierungsstatus und ihren Einsatz.

5.1.3.1.7 Risikobewertung

Ein Risiko ist die Möglichkeit, dass eine Bedrohung unter Ausnutzung einer Schwachstelle Schaden an einem Objekt oder den Verlust eines Objektes und damit direkt oder indirekt einen Schaden verursacht.

Ziel dieses Schrittes ist es, die Risiken, denen ein IT-System und seine Objekte ausgesetzt sind, zu erkennen und zu bewerten, um auf dieser Basis geeignete und angemessene Sicherheitsmaßnahmen auswählen zu können.

Risiken sind eine Funktion folgender Parameter:

- Wert der bedrohten Objekte (Schadensausmaß),
- Möglichkeit, eine Schwachstelle durch eine Bedrohung auszunutzen,
- Eintrittswahrscheinlichkeit einer Bedrohung,
- bereits existierende oder geplante Sicherheitsmaßnahmen, die dieses Risiko reduzieren könnten.

Wie diese Größen miteinander verknüpft werden, um die Höhe der Einzelrisiken und des Gesamtrisikos zu bestimmen, ist abhängig von der gewählten Risikoanalysemethode. Wieder können quantitative oder qualitative Bewertungen vorgenommen oder aber beide Möglichkeiten kombiniert werden.

Im Anhang von [ISO/IEC 27005] sind Methoden zur Risikobewertung anhand von Beispielen beschrieben.

Es ist zu beachten, dass jegliche Änderung an Werten, Bedrohungen, Schwachstellen oder Sicherheitsmaßnahmen bedeutenden Einfluss auf die Einzelrisiken und auf das Gesamtrisiko haben kann.

Ergebnis der Risikobewertung:

Quantitative oder qualitative Bewertung von Einzelrisiken und Gesamtrisiko für den betrachteten Analysebereich.

5.1.3.1.8 Auswertung und Aufbereitung der Ergebnisse

Der adäquaten Aufbereitung, Auswertung und Interpretation der Ergebnisse einer Risikoanalyse kommt wachsende Bedeutung zu. Da die Risikoanalyse auch als Grundlage für weitreichende weiterführende Entscheidungen dient, ist auf eine klare Darstellung der Situation sowie eine umfassende Ergebnisdarstellung zu achten.

Hilfreich dabei sind graphische und tabellarische Darstellungen.

5.1.4 Kombinierter Ansatz

Als dritte Alternative zu den bisher vorgestellten Risikoanalysestrategien „Grundschutzansatz“ und „Detaillierte Risikoanalyse“ wird in diesem Abschnitt der sogenannte kombinierte Ansatz beschrieben. Dieser Ansatz vereint die Vorteile aus Grundschutzansatz und detaillierter Risikoanalyse, indem die Analysetiefe abhängig vom Schutzbedarf der analysierten Objekte gemacht wird, um so mit vertretbarem Aufwand und in absehbarer Zeit bestmögliche Analyseresultate zu erzielen. In der Praxis zeigte sich, dass der kombinierte Ansatz in vielen Fällen die passendste der drei vorgestellten Risikoanalysestrategien ist.

Beim kombinierten Ansatz kommen somit die Stärken beider bisher diskutierten Risikoanalysestrategien – zeitsparende Auswahl kostengünstiger IT-Sicherheitsmaßnahmen durch Grundschutzanalysen und wirksame Reduktion hoher Sicherheitsrisiken durch detaillierte Risikoanalysen – zum Tragen.

Dabei wird zunächst ermittelt, welche IT-Systeme hohe oder sehr hohe Sicherheitsanforderungen haben, und welche niedrige bis mittlere haben (Schutzbedarfsfeststellung). Das Ergebnis dieses Schrittes ist eine Einteilung in zwei Schutzbedarfskategorien: „niedrig bis mittel“ und „hoch bis sehr hoch“.

IT-Systeme der Schutzbedarfskategorie „niedrig bis mittel“ werden einer Grundschutzanalyse unterzogen, während IT-Systeme der Schutzbedarfskategorie „hoch bis sehr hoch“ einer detaillierten Risikoanalyse zu unterziehen sind, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Alternativ dazu können auch etwa drei Schutzbedarfskategorien gewählt werden (siehe 5.1.4.1 Festlegung von Schutzbedarfskategorien, zweites Beispiel). Dabei werden IT-Systeme der Schutzbedarfskategorie „normal“ einer Grundschutzanalyse unterzogen. IT-Systeme der Schutzbedarfskategorie „hoch“ sind einer eingehenderen Betrachtung zu unterziehen. Wahlweise sind auch hier Grundschutzmaßnahmen (evtl. in verstärktem Maße) anzuwenden, oder es ist eine detaillierte Risikoanalyse durchzuführen. IT-Systeme der Schutzbedarfskategorie „sehr hoch“ sind jedenfalls einer detaillierten Risikoanalyse zu unterziehen, auf deren Basis individuelle Sicherheitsmaßnahmen ausgewählt werden.

Generell empfiehlt es sich, zunächst eine Grundschutzanalyse für alle Systeme durchzuführen und anschließend eine eventuelle erforderliche detaillierte Risikoanalyse für Systeme höherer Schutzbedarfskategorien.

Die Grundidee hinter dem kombinierten Ansatz – breite Anwendung des Grundschutzansatzes und zusätzliche Vertiefung über detaillierte Risikoanalysen in besonders kritischen Bereichen – findet sich auch in anderen einschlägigen Standards. So definiert beispielsweise der BSI-Standard 200-2 die Vorgehensweise der sogenannten Standard-Absicherung. Diese sieht ebenfalls vor, für alle relevanten Bereiche einer Organisation zunächst die Umsetzung von Standard-Sicherheitsanforderungen vorzunehmen und zusätzlich besonders schützenswerte Bereiche über eine detailliertere und aufwändigere Risikoanalyse und entsprechende Maßnahmen zu schützen.

Vorteile eines kombinierten Ansatzes sind:

- Die Vorgehensweise des kombinierten Ansatzes ermöglicht es, rasch einen relativ guten Sicherheitslevel für alle IT-Systeme zu realisieren.
- Die in der Schutzbedarfsfeststellung erarbeiteten Erkenntnisse können die Grundlage für eine Prioritätenreihung für die nachfolgenden Aktivitäten bilden.
- Der Aufwand kann auf hochsicherheitsbedürftige Systeme konzentriert werden.
- Das Verfahren findet i. Allg. hohe Akzeptanz, da es mit verhältnismäßig geringem Initialaufwand rasch sichtbare Erfolge bringt.

Aus diesen Gründen kann für die Mehrheit der Fälle empfohlen werden, als Risikoanalysestrategie einen kombinierten Ansatz zu wählen.

Wesentliche Schritte des kombinierten Ansatzes sind in Abbildung 5.7 dargestellt und werden in den folgenden Abschnitten beschrieben.

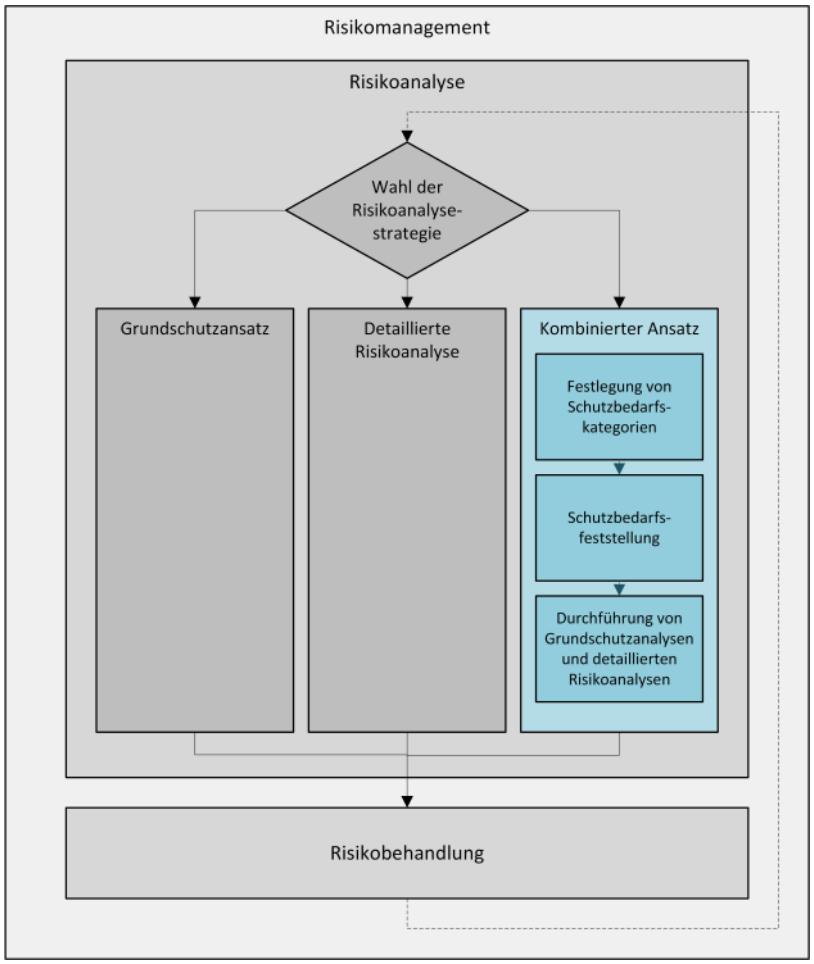

Abbildung 5.7: Wesentliche Schritte des kombinierten Ansatzes.

5.1.4.1 Festlegung von Schutzbedarfskategorien

Voraussetzung für eine Schutzbedarfsfeststellung ist die Festlegung von Schutzbedarfskategorien. Dieser Abschnitt zeigt, wie passende Schutzbedarfskategorien festgelegt werden können.

Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der Schutzbedarfskategorien und damit die Klassifizierung der Anwendungen anhand der maximal möglichen Schäden anhand von Grenzwerten. Diese sind jedoch nur als Beispiele zu verstehen. Jede Organisation sollte für sich prüfen, ob diese Klassifizierung ihren Anforderungen entspricht und gegebenenfalls eigene Grenzwerte und Einordnungen festlegen.

Weiters ist darauf hinzuweisen, dass die in der Tabelle angeführten sieben Schadenskategorien nicht vollständig sein müssen. Für alle Schäden, die sich nicht in diesen Kategorien abbilden lassen, ist ebenfalls eine Aussage zu treffen, wo die Grenze zwischen „niedrig bis mittel“ und „hoch bis sehr hoch“ zu ziehen ist.

	Kategorie „niedrig bis mittel“	Kategorie „hoch bis sehr hoch“
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Verletzungen von Verträgen mit geringen Konventionalstrafen • Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/ des Betroffenen	• Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung) • Verletzungen von Verträgen mit hohen Konventionalstrafen oder Haftungsschäden • Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen (Verlust der Vertraulichkeit oder Integrität sensibler Daten)
2. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.	• Eine über Bagatellverletzungen hinausgehende Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
3. Beeinträchtigung der Aufgabenerfüllung	• Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen. • Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich.	• Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen. • Bedeutende Zielabweichung in Qualität oder Quantität.
4. Vertraulichkeit der verarbeiteten Information	• Es werden nur Daten der Sicherheitsklassen OFFEN und EINGESCHRÄNKT verarbeitet bzw. gespeichert.	• Es werden auch Daten der Sicherheitsklassen VERTRAULICH, GEHEIM oder STRENG GEHEIM verarbeitet bzw. gespeichert.
5. Dauer der Verzichtbarkeit	• Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehrere Stunden bis mehrere Tage.	• Die maximal tolerierbare Ausfallszeit des Systems beträgt lediglich einige Minuten.
6. Negative Außenwirkung	• Eine geringe bzw. nur interne Beeinträchtigung des Ansehens oder Vertrauens ist zu erwarten.	• Eine breite Beeinträchtigung des Vertrauens in die Organisation oder ihr Ansehen ist zu erwarten.
7. Finanzielle Auswirkungen	• Der finanzielle Schaden ist kleiner als (z. B.) EUR 50.000.--.	• Der zu erwartende finanzielle Schaden ist größer als (z. B.) EUR 50.000.--.

Tabelle 5.1: Beispiel für die Festlegung der Schutzbedarfskategorien

Eine andere Möglichkeit besteht darin, drei Schutzbedarfskategorien zu definieren:

- Schutzbedarfskategorie „normal“:

Die Schadensauswirkungen sind begrenzt und überschaubar. Maßnahmen des IT-Grundschutzes reichen i. Allg. aus. Diese Kategorie entspricht der obigen Kategorie „niedrig bis mittel“.

- Schutzbedarfskategorie „hoch“:
  Die Schadensauswirkungen können beträchtlich sein. Wahlweise können weiter (verstärkte) Grundschutzmaßnahmen eingesetzt oder eine detaillierte Risikoanalyse durchgeführt werden.
- Schutzbedarfskategorie „sehr hoch“:
  Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. IT-Grundschutzmaßnahmen alleine reichen nicht aus, die erforderlichen Sicherheitsmaßnahmen sollten individuell auf Basis einer Risikoanalyse ermittelt werden.

Die nachfolgende Tabelle gibt eine Orientierungshilfe für die Festlegung der Schutzbedarfskategorien und damit die Klassifizierung der Anwendungen anhand der oben angeführten Einteilungen. Diese sind wiederum als Beispiele zu sehen. Jede Organisation sollte für sich prüfen, ob diese Klassifizierung ihren Anforderungen entspricht und gegebenenfalls eigene Grenzwerte und Einordnungen festlegen.

	Kategorie „normal“	**Kategorie „hoch“**	**Kategorie „sehr hoch“**
1. Verstoß gegen Gesetze, Vorschriften oder Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen. • Geringfügige Verletzungen von Verträgen mit keinen oder geringen Konventionalstrafen. • Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen.	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen. • Verletzungen von Verträgen mit hohen Konventionalstrafen. • Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen.	• Schwere Verstöße gegen Gesetze und Vorschriften (Strafverfolgung). • Verletzungen von Verträgen, deren Haftungsschäden ruinös sind. • Ein möglicher Missbrauch personenbezogener Daten würde für die Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
2. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben.

	Kategorie „normal“	Kategorie „hoch“	Kategorie „sehr hoch“
3. Beeinträchtigung der Aufgabenerfüllung	• Es kann zu einer leichten bis maximal mittelschweren Beeinträchtigung der Aufgabenerfüllung kommen. • Eine Zielerreichung ist mit vertretbarem Mehraufwand möglich.	• Es kann zu einer schweren Beeinträchtigung der Aufgabenerfüllung kommen. • Bedeutende Zielabweichung in Qualität oder Quantität.	• Es kann zu einer sehr schweren Beeinträchtigung der Aufgabenerfüllung bis hin zur Handlungsunfähigkeit der betroffenen Organisation kommen.
4. Vertraulichkeit der verarbeiteten Information	• Es werden nur Daten der Sicherheitsklassen OFFEN und EINGESCHRÄNKT verarbeitet bzw. gespeichert.	• Es werden auch Daten der Klasse VERTRAULICH verarbeitet bzw. gespeichert.	• Es werden auch Daten der Klassen GEHEIM oder STRENG GEHEIM verarbeitet bzw. gespeichert.
5. Dauer der Verzichtbarkeit	• Die maximal tolerierbare Ausfallszeit der Anwendung beträgt mehr als 24 Stunden.	• Die maximal tolerierbare Ausfallszeit des Systems liegt zwischen einer und 24 Stunden.	• Die maximal tolerierbare Ausfallszeit des Systems ist kleiner als eine Stunde.
6. Negative Außenwirkung	• Eine geringe bzw. nur interne Beeinträchtigung des Ansehens oder Vertrauens ist zu erwarten.	• Eine breite Beeinträchtigung des Ansehens oder Vertrauens ist zu erwarten.	• Eine landesweite breite Ansehens- oder Vertrauens-beeinträchtigung, evtl. sogar existenzgefährdender Art, ist zu erwarten.
7. Finanzielle Auswirkungen	• Der finanzielle Schaden liegt unter (z. B.) EUR 50.000.--.	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabelle 5.2: Beispiel für die alternative Festlegung der Schutzbedarfskategorien

5.1.4.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung bildet die Grundlage für eine Entscheidung über die weitere Vorgehensweise und ist daher mit entsprechender Sorgfalt durchzuführen.

Die Schutzbedarfsfeststellung erfolgt in drei Schritten:

- Schritt 1: Erfassung aller vorhandenen oder geplanten IT-Systeme

- Schritt 2: Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen
- Schritt 3: Schutzbedarfsfeststellung für jedes IT-System

5.1.4.2.1 Erfassung aller vorhandenen oder geplanten IT-Systeme

Zunächst werden die vorhandenen und geplanten IT-Systeme aufgelistet. Hierbei steht die technische Realisierung eines IT-Systems im Vordergrund, z. B. Stand-Alone-PC, Server, PC-Client, Windows-Server. An dieser Stelle soll nur das System als solches erfasst werden (z. B. Windows-Server), nicht die einzelnen Bestandteile, wie Rechner, Tastatur, Bildschirm, Drucker etc., aus denen das IT-System zusammengesetzt ist.

Zur Reduktion der Komplexität kann man gleiche IT-Systeme zu Gruppen zusammenfassen, wenn von Anwendungsstruktur und -ablauf vergleichbare Anwendungen auf diesen Systemen laufen. Dies gilt insbesondere für PCs, die oft in großer Anzahl vorhanden sind („Sekretariats-PCs“).

5.1.4.2.2 Erfassung der IT-Anwendungen und Zuordnung zu den einzelnen IT-Systemen

Ziel dieses Schrittes ist es, alle oder zumindest die wichtigsten auf dem betrachteten IT-System laufenden oder geplanten IT-Anwendungen zu erfassen.

Diese sollten anschließend - soweit zu diesem Zeitpunkt bereits möglich - nach ihrem Sicherheitsbedarf vorsortiert werden. Dabei sind zuerst diejenigen Anwendungen des jeweiligen IT-Systems zu benennen,

- deren Daten/Informationen und Programme den höchsten Bedarf an Vertraulichkeit haben,
- deren Daten/Informationen und Programme den höchsten Bedarf an Integrität aufweisen,
- die die kürzeste tolerierbare Ausfallszeit haben.

5.1.4.2.3 Schutzbedarfsfeststellung für jedes IT-System

In dieser Phase soll die Frage beantwortet werden, welche Schäden zu erwarten sind, wenn Vertraulichkeit, Integrität oder Verfügbarkeit einer IT-Anwendung oder der zugehörigen Informationen ganz oder teilweise verloren gehen. Die zu erwartenden Schäden bestimmen den Schutzbedarf. Dabei ist es unbedingt auch erforderlich, die Applikations-/Projektverantwortlichen und die BenutzerInnen der betrachteten IT-Anwendungen nach ihrer Einschätzung zu befragen.

Als Orientierungshilfe für die Einordnung von IT-Anwendungen in Schutzbedarfskategorien kann die in 5.1.4.1 Festlegung von Schutzbedarfskategorien angeführte Tabelle dienen. Es ist aber empfehlenswert, eine den spezifischen Anforderungen der betroffenen Organisation entsprechende modifizierte Tabelle zu erstellen.

Die Ermittlung des Schutzbedarfes erfolgt nach dem Maximum-Prinzip. Ist für alle auf einem System laufenden Anwendungen ein normaler Schutzbedarf erhoben worden, so ist das gesamte System in die Schutzbedarfskategorie „normal“ einzuordnen. Die Realisierung von Grundschutzmaßnahmen bietet hier in der Regel einen ausreichenden Schutz. Wurde dagegen mindestens eine Applikation mit hohem oder sehr hohem Schutzbedarf ermittelt, so ist das gesamte IT-System in die Schutzbedarfskategorie „hoch“ bzw. „sehr hoch“ einzuordnen.

5.1.4.3 Durchführung von Grundschutzanalysen und detaillierten Risikoanalysen

Für alle IT-Systeme der Schutzbedarfskategorie „niedrig bis mittel“ bzw. „normal“ ist eine Grundschutzanalyse gemäß der in 5.1.2 Grundschutzansatz beschriebenen Vorgehensweise durchzuführen.

Alle IT-Systeme der Schutzbedarfskategorie „hoch bis sehr hoch“ sind einer detaillierten Risikoanalyse zu unterziehen. Die Auswahl einer konkreten Methode zur Risikoanalyse sowie der eventuelle Einsatz eines Tools zur Unterstützung dieser Analyse bleiben der durchführenden Institution überlassen. Details dazu finden sich in 5.1.3 Detaillierte Risikoanalyse.

Geht man von drei Schutzbedarfskategorien aus, so ist für IT-Systeme der Schutzbedarfskategorie „hoch“ zu überlegen, ob mit (evtl. verstärkten) Grundschutzmaßnahmen das Auslangen gefunden werden kann, oder eine detaillierte Risikoanalyse erforderlich ist. IT-Systeme der Schutzbedarfskategorie „sehr hoch“ sind jedenfalls einer detaillierten Risikoanalyse zu unterziehen.

5.2 Risikobehandlung

Neben der Risikoanalyse stellt die Risikobehandlung den zweiten elementaren Baustein eines erfolgreichen Risikomanagements dar. Im Rahmen der Risikoanalyse wird versucht, bestehende Risiken die Organisation und ihre IT-Systeme betreffend möglichst vollständig zu identifizieren und zu bewerten. Die Risikobehandlung baut auf den Ergebnissen der Risikoanalyse auf und versucht identifizierte und bewertete Risiken bestmöglich zu adressieren.

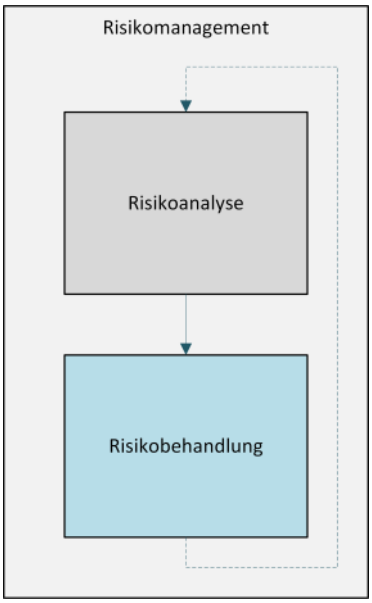

Abbildung 5.8: Rolle der Risikobehandlung im Risikomanagement.

Hierzu beschreibt dieser Abschnitt mögliche Strategien im Umgang mit identifizierten Risiken sowie Methoden zur Auswahl und Umsetzung geeigneter Maßnahmen, über die identifizierte Risiken adressiert werden können.

Die hier beschriebene Risikobehandlung ist auch unmittelbar relevant für die Anwendung von Risikomanagementmethoden im Rahmen der NIS2-Verordnung. Diese definiert unter anderem den Einsatz von Sicherheitsmaßnahmen (z.B. Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT, Multi-Faktor-Authentifizierung oder auch Kryptografie und ggf. Verschlüsselung) zur Erhöhung der Sicherheit kritischer Systeme. Weitere Details finden sich unter 5.4.2 Risikomanagement im Kontext der NIS2-Richtlinie.

Die Inhalte dieses Abschnitts orientieren sich an einschlägigen Standards und Normen wie z. B. BSI-Standards 200-2 und 200-3 oder auch ISO/IEC 27005. Dieser Abschnitt fasst Handlungsanweisungen und Empfehlungen zur Risikobehandlung aus diesen Standards und Normen zusammen und bietet so einen möglichst umfangreichen Leitfaden zum erfolgreichen Umgang mit Risiken.

5.2.1 Strategien zum Umgang mit Risiken

Nach erfolgter Identifizierung und Bewertung eines Risikos stellt sich unmittelbar die Frage nach einer geeigneten Vorgehensweise zur Adressierung dieses Risikos. Mögliche Strategien zum Umgang mit identifizierten Risiken lassen sich in vier Kategorien gliedern. Diese sind in den folgenden Unterabschnitten beschrieben.

5.2.1.1 Risikovermeidung

Die Strategie der Risikovermeidung beschreibt jene Ansätze der Risikobehandlung, in denen das betreffende Risiko – z.B. durch Umstrukturierung von Geschäftsprozessen oder IT-Systemen – gänzlich vermieden wird. Beispielsweise könnte ein von einer Schwachstelle betroffenes IT-System aus der IT-Infrastruktur der Organisation entfernt werden, sodass sich das in der Schwachstelle begründete Risiko erst gar nicht manifestieren kann.

Die Strategie der Risikovermeidung ist zumeist sehr wirksam, kann in der Praxis aber nicht immer verfolgt werden. Betrifft die im obigen Beispiel erwähnte Schwachstelle ein für die Geschäftsprozesse der Organisation hochrelevantes IT-System, kann dieses zumeist nicht einfach ersatzlos aus der IT-Infrastruktur entfernt werden. Vor Erwägung anderer Strategien sollte aber jedenfalls geprüft werden, ob das identifizierte Risiko grundlegend vermieden werden kann.

5.2.1.2 Risikoreduzierung

Der Begriff Risikoreduzierung fasst all jene Ansätze zusammen, durch die ein identifiziertes Risiko über die Implementierung zusätzlicher oder die Erweiterung bestehender Sicherheitsmaßnahmen reduziert wird. Diese Sicherheitsmaßnahmen können technischer und/oder organisatorischer Natur sein. Beispielsweise kann das Risiko eines Datenverlusts durch Hardware-Defekte über die Implementierung zusätzlicher Backup-Mechanismen reduziert werden.

In der Regel können für jedes Risiko geeignete technische oder organisatorische Maßnahmen gefunden werden, die diesem Risiko effektiv entgegenwirken. Kritisch ist dabei in der Regel der mit der Umsetzung dieser Maßnahmen verbundene personelle und finanzielle Aufwand. Hier gilt es spezifisch abzuwägen, ob die Adressierung eines Risikos durch Umsetzung zusätzlicher bzw. Erweiterung bestehender Sicherheitsmaßnahmen die ideale Strategie darstellt.

5.2.1.3 Risikotransfer

Kann ein identifiziertes Risiko weder sinnvoll vermieden noch mit vertretbarem Aufwand reduziert werden, bietet sich ein Risikotransfer an. Grundidee hinter dieser Strategie ist es, das bestehende Risiko an eine externe Stelle zu transferieren. Dies ist in der Regel mit finanziellem Aufwand verbunden.

Ein Beispiel eines Risikotransfers ist der Abschluss einer Versicherung, um sich gegen Schäden aus der Materialisierung eines Risikos zu schützen. Ein anderes Beispiel wäre das Outsourcing einer von einem identifizierten Risiko betroffenen Komponente an einen externen Dienstleister.

Nicht alle identifizierten Risiken können sinnvoll an externe Stellen transferiert werden. Während z. B. finanzielle Schäden in der Regel gut über Versicherungen abgefangen werden können, ist dies bei Beschädigung der eigenen Reputation kaum möglich. Risiken, die zu derartige Schäden führen können, sind daher oft nur schwer transferierbar.

5.2.1.4 Risikoakzeptanz

In der Praxis werden sich immer wieder Risiken ergeben, für die keine der drei bisher genannten Strategien zielführend scheint. Dies betrifft beispielsweise Risiken, die weder vermeidbar noch transferierbar sind, deren Reduzierung aber zusätzlicher Maßnahmen bedürfe, deren Umsetzung die Möglichkeiten der Organisation übersteigt. Punktuell können sich auch Risiken ergeben, für die aktuell noch keine Gegenmaßnahmen bekannt sind.

Für solche Fälle kann es der praktikabelste Ansatz sein, das Risiko zu akzeptieren. Dies bietet sich vor allem für Risiken an, deren Eintrittswahrscheinlichkeit sehr gering ist. Die Entscheidung über die Akzeptanz eines Risikos ist durch das Management zu treffen, die genauen Verantwortlichkeiten dafür sind in der Informationssicherheitspolitik festzulegen. Die Entscheidung ist schriftlich zu begründen und durch die Leitung der Organisation in schriftlicher Form zu akzeptieren.

5.2.2 Auswahl von Maßnahmen

Abhängig von den gewählten Strategien zum Umgang mit identifizierten Risiken, wird es in der Regel notwendig sein, geeignete Maßnahmen zur Adressierung dieser Risiken zu finden. In englischsprachigen Standards (z.B. ISO/IEC 27005) werden solche Maßnahmen oft auch als „Controls“ bezeichnet.

Ausgehend von einer bestehenden Liste identifizierter Risiken ist es das Ziel, für jedes Risiko unter Berücksichtigung der gewählten Strategie zum Umgang mit diesem Risiko eine oder mehrere geeignete Maßnahmen auszuwählen, um dem Risiko entsprechend zu begegnen. Da die Umsetzung von Maßnahmen in der Regel mit Aufwand verbunden ist, sollen nur solche Maßnahmen ausgewählt werden, die einen nichtvernachlässigbaren Effekt auf das jeweilige Risiko haben.

Zur Auswahl geeigneter Maßnahmen stehen diverse Kataloge zur Verfügung (z.B. ISO/IEC 27001 – Annex A, BSI IT-Grundschutz-Kompendium, etc.). Eine Orientierung an solchen Katalogen ist empfehlenswert, da diese Maßnahmen in der Regel vollständig und gut dokumentiert bereitstellen.

Im Allgemeinen lassen sich Maßnahmen in drei Kategorien unterteilen:

- **Präventive Maßnahmen:** Diese Maßnahmen reduzieren die Wahrscheinlichkeit, dass sich ein Risiko materialisiert.
- **Detektierende Maßnahmen:** Diese Maßnahmen erkennen die Materialisierung eines Risikos (z.B. Sicherheitsvorfall).
- **Korrigierende Maßnahmen:** Diese Maßnahmen limitieren die negativen Konsequenzen eines bereits materialisierten Risikos.

Im Zuge der Auswahl von Maßnahmen muss sichergestellt werden, dass jedes identifizierte Risiko über eine oder mehrere ausgewählte Maßnahmen ausreichend adressiert ist. In der Praxis empfiehlt sich hier die tabellarische Gegenüberstellung von Risiken und zugeordneten Maßnahmen. Über eine solche Gegenüberstellung kann die vollständige Abdeckung aller Risiken evaluiert werden. Für komplexe und umfangreiche Risikomanagementszenarien, die eine Vielzahl an Risiken und Maßnahmen umfassen, kann auch die Verwendung einschlägiger Tools zur Erfassung und Gegenüberstellung von Risiken und Maßnahmen angedacht werden.

5.2.3 Umsetzung von Maßnahmen

Wurden notwendige Maßnahmen vollständig ausgewählt, sodass alle zuvor identifizierten Risiken ausreichend adressiert sind, müssen die ausgewählten Maßnahmen schlussendlich zur Umsetzung gebracht werden. Die Umsetzung aller relevante Maßnahmen kann ein komplexes und längerfristiges Unterfangen sein. Es empfiehlt sich daher, dieses Vorhaben gut zu planen und zu dokumentieren. Einschlägige Standards wie ISO/IEC 27005 sehen dafür die Erstellung spezifischer Planungsdokument (z.B. Risk Treatment Plan nach ISO/IEC 27005) vor.

In der Erstellung solcher Planungsdokumente sollten unter anderem die folgenden Aspekte berücksichtigt werden:

- **Prioritäten:** Priorisierung der Maßnahmenumsetzung unter Berücksichtigung der Höhe der Risiken, die über die jeweiligen Maßnahmen adressiert werden
- **Abhängigkeiten:** Identifizierung von Abhängigkeiten zwischen verschiedenen Maßnahmen, die deren Umsetzung beeinflussen können
- **Aktionspunkte:** Spezifikation der konkreten Aktionspunkte zur Umsetzung der geplanten Maßnahmen

- **Durchlaufzeiten:** Abschätzung von Durchlaufzeiten bis zur effektiven Einsatzbereitschaft der umgesetzten Maßnahmen
- **Ressourcen:** Abschätzung notwendiger personeller und finanzieller Ressourcen zur Umsetzung geplanter Maßnahmen
- **Verantwortlichkeiten:** Definition der für die Umsetzung und Freigabe der notwendigen Maßnahmen verantwortlichen Personen oder Rollen

Nicht nur die Planung, auch die Umsetzung notwendiger Maßnahmen selbst sollte über entsprechende Dokumentationen begleitet werden. Diese sollten unter anderem so gestaltet sein, dass sie ein Reporting und Monitoring im Zusammenhang mit den jeweiligen Umsetzungsaktivitäten ermöglichen und vereinfachen.

5.2.4 Umgang mit Restrisiken

Sicherheitsmaßnahmen können für gewöhnlich Risiken nur teilweise mindern. Im Allgemeinen verbleibt ein Restrisiko, dessen Abdeckung wirtschaftlich nicht mehr vertretbar wäre. Es ist notwendig, diese Restrisiken so exakt wie möglich zu quantifizieren und sie dann bewusst zu akzeptieren.

Um ein organisationsweit einheitliches Niveau des Restrisikos zu gewährleisten, ist es hilfreich, diesen Prozess durch generelle Richtlinien zu unterstützen. Diese sollten im Rahmen der Informationssicherheitspolitik definiert werden und festlegen, welche Risiken die betroffene Organisation generell zu akzeptieren bereit ist.

Dabei ist zu beachten, dass durch Kumulationseffekte oder gegenseitige Beeinflussungen eine Reihe von kleinen Einzelrisiken zu einem inakzeptablen Restrisiko führen kann.

Die Entscheidung über die Akzeptanz von Restrisiken ist daher immer eine für das spezielle System zu treffende Managemententscheidung.

5.2.5 Maßnahmenbewertung

Geplante, umgesetzte und ausgerollte Maßnahmen müssen laufend in Bezug auf ihre Wirksamkeit bewertet werden. Dazu sollten in der Maßnahmenplanung bereits entsprechende Leistungsindikatoren definiert werden, anhand derer die entsprechenden Maßnahmen zu einem späteren Zeitpunkt evaluiert werden können. Nicht oder zu wenig wirksame Maßnahmen müssen dabei laufend verbessert werden. Die iterative Natur des gesamten Risikomanagementprozesses unterstützt dabei, da bestehende Maßnahmen im Zuge von wiederkehrenden Risikoanalysen regelmäßig geprüft werden.

5.3 Praktische Herausforderungen und Strategien

Der Überblick zu relevanten Aspekten des Risikomanagements, der in diesem Kapitel bisher gegeben wurde, zeigt, dass verfügbare Normen und Standards anzuwendende Methoden umfangreich und vollständig definieren und beschreiben. In der Praxis zeigt sich jedoch, dass die konkrete Umsetzung dieser Methoden oft schwierig ist und verantwortliche Personen vor Herausforderungen stellt, die über die einschlägigen Normen und Standards nicht immer ausreichend adressiert sind. Dieser Abschnitt gibt daher einen Überblick über mögliche Herausforderungen, die sich in der praktischen Umsetzung von Risikomanagementmethoden ergeben können und bietet dafür Lösungsstrategien und Empfehlungen.

Detailgrad und Komplexität

Die in der Praxis oft größte Herausforderung im Rahmen des Risikomanagements ist die Beherrschung der Komplexität. Diese ergibt sich vor allem in der Risikoanalyse und ist in dem Ziel begründet, einen möglichst hohen Grad an Vollständigkeit zu erreichen, d.h. möglichst alle bestehenden Risiken zu identifizieren. Entsprechend der üblichen Vorgehensweise werden Risiken systematisch aus Bedrohungen und Assets (Werten, Objekten) abgeleitet.

Um Risiken vollständig zu identifizieren, müssen demnach zunächst auch Assets und deren Bedrohungen vollständig identifiziert worden sein. In der Praxis wird dazu ein Modell der zu analysierenden Organisation (bzw. des definierten Geltungsbereichs) erstellt, das alle relevanten Assets und deren Abhängigkeiten enthält (siehe z. B. Strukturanalyse laut BSI-Standard 200-2). In detaillierten Modellierungen enthält das erstellte Modell auch die Schutzbedarfe der enthaltenen Assets und setzt Assets zudem in Verbindung zu relevanten Geschäftsprozessen der Organisation.

Wurden alle Assets entsprechend modelliert, können für jedes Asset relevante Bedrohungen systematisch und damit vollständig identifiziert werden. Über die modellierten Abhängigkeiten zwischen Assets wird auch ersichtlich, wie sich Bedrohungen auf die Sicherheit abhängiger Assets und verbundener Geschäftsprozesse auswirken. Aus der Modellierung von Assets und Bedrohungen können schlussendlich relevante Risiken abgeleitet werden.

Vor allem für große Organisationen oder breit gefasste Geltungsbereiche innerhalb dieser Organisationen können Modellierungen relevanter Assets und Bedrohungen rasch umfangreich und komplex werden. Dies betrifft damit insbesondere mittlere und große Organisationen, für die auch die NIS2-Richtlinie speziell relevant ist. Die sich ergebende Komplexität bringt mehrere Herausforderungen mit sich:

- Der Aufwand für die initiale Erstellung des Modells ist sehr hoch.

- Modellierungsarbeiten lassen sich nur beschränkt parallelisieren, wodurch mit steigendem Aufwand für komplexer werdende Modelle in der Regel auch die Durchlaufzeiten steigen. Dadurch sind Resultate aus Risikoanalysen erst später verfügbar und aktuelle Risiken bleiben so länger unentdeckt.
- Lange Durchlaufzeiten in der Modellierung stellen auch für sich eine Herausforderung dar. Da eine Organisation und ihre Prozesse und Assets laufenden Änderungen unterworfen sind, müssen Modelle bereits im Zuge ihrer initialen Erstellung mehrfach angepasst werden. Je länger die Durchlaufzeit in der Modellerstellung, desto mehr Anpassungen sind hier notwendig. Das wirkt sich wiederum auf die Durchlaufzeit negativ aus.
- Hochkomplexe Modelle machen auch die laufende Wartung der Modelle (regelmäßige Anpassungen an geänderte Realitäten, etc.) aufwändiger.

Mit steigender Komplexität in der Modellierung ergeben sich somit zunehmend Nachteile, die ab einem gewissen Punkt durch den höheren Detailgrad des Modells nicht mehr gerechtfertigt werden können. In der Praxis ist es daher empfehlenswert, den Detailgrad des Modells und damit die Komplexität der Modellierung zu beschränken. Eine Methode dazu ist z.B. die im BSI-Standard 200-2 beschriebene Methode der Gruppenbildung, über die Assets mit ähnlichen Eigenschaften zu Gruppen zusammengefasst werden und somit nur einmal modelliert und betrachtet werden müssen. Die Gruppenbildung ist damit eine Form der Abstrahierung, über die die Komplexität eines Modells reduziert werden kann.

Während mit zunehmender Abstrahierung die Komplexität des Modells und der Aufwand der Modellierungsarbeit sinkt, steigt in gleichem Maße die Gefahr, dass bestimmte Details (z.B. spezifische Bedrohungen für spezielle Assets) aus dem Modell nicht mehr ersichtlich werden und dadurch die Vollständigkeit des Modells in Bezug auf identifizierte Assets und Bedrohungen sinkt. Damit steigt die Gefahr, relevante Risiken zu übersehen. Im Allgemeinen erlaubt ein abstrakteres Modell auch nur allgemeinere und ungenauere Aussagen zu Bedrohungen und Risiken als ein detailliertes Modell.

In der Praxis ergibt sich damit die Herausforderung, einen für die Modellierung passenden Abstraktionsgrad zu finden. Dieser bewegt sich stets im Spannungsfeld zwischen Vollständigkeit/Detailgrad und Komplexität. Unglücklicherweise kann für die Wahl eines passenden Abstraktionsgrads kein allgemeingültiges Patentrezept angegeben werden. Die Wahl des passendes Abstraktionsgrads ist unter anderem abhängig von den folgenden Faktoren:

- **Verfügbare Ressourcen:** Die Erstellung und laufende Wartung eines Modells der Organisation ist eine ressourcenintensive Aufgabe. Je komplexer das Modell, desto aufwändiger seine Erstellung und spätere Wartung. Die Wahl des Abstraktionsgrads ist dadurch automatisch limitiert durch die zur Verfügung

stehenden Ressourcen. Je mehr Ressourcen zur Verfügung stehen, desto detaillierter kann die Modellierung ausfallen. Dies bedeutet jedoch nicht automatisch, dass immer der mit den vorhandenen Ressourcen maximal erreichbare Detailgrad angestrebt werden muss.

- **Umfang und Komplexität der Organisation/des Geltungsbereichs:** Je größer und komplexer die zu modellierendende Organisation bzw. der definierte Geltungsbereich, desto weniger detailliert und desto abstrakter muss bei konstanten verfügbaren Ressourcen deren Modellierung ausfallen.
- **Heterogenität der Organisation/des Geltungsbereichs:** Je heterogener die zu modellierende Organisation bzw. der definierte Geltungsbereich, desto schwieriger können abstrahierende Konzepte wie Gruppenbildung zur Anwendung kommen und desto detaillierter muss eine Modellierung ausfallen, um die erwünschten Resultate zu erhalten.
- **Weitere individuelle Eigenschaften der Organisation/des Geltungsbereichs:** Es können noch zusätzliche Eigenschaften der Organisation/des Geltungsbereichs existieren, die die Wahl des passenden Abstraktionsgrads einer Modellierung beeinflussen können. In jedem Fall sollte diese Wahl daher situationsspezifisch und abhängig von den Eigenschaften der zu modellierenden Organisation/des zu modellierenden Geltungsbereichs erfolgen.

Verwendung von Tools

Eine Möglichkeit, den Herausforderungen überbordender Komplexität zu begegnen, ist der Einsatz einschlägiger Tools. Am Markt existieren diverse Tools, die bei Aufgaben im Rahmen des Risikomanagements unterstützen. Unter anderem erlauben solche Tools die Modellierung von Organisation bzw. definierten Geltungsbereichen. In vielen Fällen stellen diese Tools dafür vorgefertigte Bausteine zur Verfügung, die den Modellierungsprozess unterstützen. In der Regel sind diese Bausteine auch mit Katalogen zu Bedrohungen und Maßnahmen verknüpft, wodurch der Einsatz dieser Tools die Vollständigkeit der Modellierung unterstützt.

Während verfügbare Tools somit bei der Beherrschung der Komplexität und der Erreichung eines höchstmöglichen Grades an Vollständigkeit unterstützen können, dürfen diese nicht als Allheilmittel gesehen werden. Auch durch den erfolgreichen Einsatz einschlägiger Tools kann das Problem überbordende Komplexität in der Modellierung nicht vollständig gelöst werden. Bei Verwendung eines Tools tritt dieses Problem in der Regel aber erst später – d.h. ab einem höheren Detailgrad – auf. Geeignete Tools erlauben somit detailliertere Modellierungen, die Herausforderung der Wahl eines geeigneten Abstraktionsgrads für die Modellierung bleibt aber prinzipiell bestehen. Die praktische Erfahrung zeigt, dass auch die toolbasierte Modellierung oft ein iterativer – und damit zeitintensiver – Prozess ist, über den eine Annäherung an den idealen Abstraktionsgrad erfolgt.

Es wird an dieser Stelle daher bewusst keine Empfehlung für oder gegen die Verwendung einschlägiger Tools gegeben. Die Sinnhaftigkeit eines Einsatzes ist stark situations- und kontextabhängig und sollte daher stets individuell und unter Abwägung der spezifischen Vor- und Nachteile geprüft werden. Dies betrifft nicht nur die generelle Entscheidung für oder gegen den Einsatz eines einschlägigen Tools.

Fällt die Entscheidung für den Einsatz eines Tools, ist auch die Wahl des bestgeeigneten Tools von entscheidender Bedeutung. Dabei ist zu beachten, dass sich verfügbare Tools in diversen Eigenschaften unterscheiden. So implementiert jedes Tool in der Regel eine spezifische Risikomanagementmethode, die sich in Details von implementierten Methoden anderer Tools unterscheidet. Mit der Auswahl eines Tools verpflichtet man sich damit auch implizit, der spezifischen Risikomanagementmethode des gewählten Tools zu folgen.

Zusätzlich verfügt jedes Tool über spezifische Stärken und Schwächen, die je nach Anwendungskontext unterschiedlich stark zutage treten können. Auch zu beachten ist, dass der spätere Umstieg auf ein anderes Tool in den meisten Fällen nur mit großem Aufwand möglich ist und im schlimmsten Fall die erneute Modellierung der Organisation bzw. des relevanten Geltungsbereichs bedingt. Die Entscheidung für oder gegen den Einsatz einschlägiger Tools und die Auswahl eines konkreten Tools sollten daher stets sorgfältig und unter Abwägung aller genannten Faktoren erfolgen.

Empfehlungen

In der praktischen Durchführung von Risikomanagement und seiner Kernelemente Risikoanalyse und Risikobehandlung ergeben sich zahlreiche Herausforderungen, deren Ursache primär in der den zugrundliegenden Methoden inhärenten Komplexität begründet ist. Zur Bewältigung dieser Herausforderungen können zusammenfassend folgende Empfehlungen gegeben werden:

- **Wahl eines geeigneten Abstraktionsgrads:** Die Wahl eine geeigneten Abstraktionsgrads für Modellierungen im Rahmen des Risikomanagements ist eine wesentliche Grundvoraussetzung. Der Abstraktionsgrad sollte in Abhängigkeit der spezifischen Rahmenbedingungen so gewählt werden, dass mit den verfügbaren Ressourcen bestmögliche Ergebnisse erzielt werden können.
- **Iteratives Vorgehen:** Es ist vor allem bei wenig Vorerfahrung nicht unwahrscheinlich, dass sich der initial gewählte Abstraktionsgrad als unpassend erweist. Modellierungen im Rahmen der Risikoanalyse sollten daher als iterativer Prozess verstanden werden, über den schrittweise eine Annäherung an den idealen Abstraktionsgrad erfolgt. Im Allgemeinen ist es ressourcenschonender und daher empfehlenswert, mit einem höheren Abstraktionsgrad zu starten.

- **Realistische Aufwandsabschätzungen:** Es sollte berücksichtigt werden, dass der gewählte Abstraktionsgrad nicht nur den Aufwand der initialen Erstellung des Modells der Organisation bzw. des relevanten Geltungsbereichs beeinflusst, sondern auch Auswirkungen auf die laufende Wartung und Pflege des Modells hat. Je höher der Detailgrad, desto aufwändiger die laufende Wartung und desto höher die mit der Wartung verbundenen Aufwände.
- **Bewusste Entscheidungen bezüglich der Verwendung von Tools:** Die Verwendung einschlägiger Tools kann bei der Beherrschung komplexer Modelle helfen und so detailliertere Modelle und damit genauere Analyseergebnisse ermöglichen. Die Verwendung von Tools unterliegt aber auch diversen Einschränkungen und kann auch Nachteile mit sich bringen. Ob und welches Tool am besten zum Einsatz kommen soll, hängt von den spezifischen Rahmenbedingungen ab und sollte daher stets eine bewusste und informierte Entscheidung sein.
- **Verwendung von Katalogen:** Zur Erhöhung der Vollständigkeit durchgeführter Risikoanalysen empfiehlt sich die Verwendung von Katalogen, die z.B. relevante Bedrohungen für Asset-Klassen auflisten. Bei Verwendung einschlägiger Tools werden solche Kataloge oft über diese Tools bereitgestellt. Auch wenn auf die Verwendung einschlägiger Tools verzichtet wird, ist die Verwendung von Katalogen empfehlenswert.

5.4 Ausgewählte Anwendungsfälle des Risikomanagements

Um Betrachtungen zum Thema Risikomanagement abzurunden, beleuchtet dieser Abschnitt ausgewählte Anwendungsfälle, in denen Konzepte des Risikomanagements zur Anwendung kommen.

Konkret werden im Folgenden zwei Anwendungsfälle beschrieben. Abschnitt 5.4.1 geht zunächst auf die Erstellung von Datenschutzfolgenabschätzungen im Kontext der DSGVO ein und zeigt, welche Methoden dort zur Anwendung kommen, um datenschutzspezifische Risiken vorab zu identifizieren. Im Anschluss daran widmet sich Abschnitt 5.4.2 der NIS2-Richtlinie und beleuchtet auch für diese notwendige Konzepte der Risikoanalyse.

5.4.1 Datenschutz-Folgenabschätzung

Die Behandlung von Datenschutzrisiken muss integraler Bestandteil der genannten Risikoanalysestrategien sein. Mit der Datenschutzgrundverordnung (DSGVO) wird in bestimmten Fällen auch die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) notwendig (vgl. Artikel 35 DSGVO).

Eine DSFA verfolgt die drei Ziele:

1. Erfüllen der Anforderungen „data protection by design“ und „data protection by default“
2. Risikobasiertes ableiten von organisatorischen bzw. technischen Schutzfunktionen
3. Schaffen von Transparenz der jeweiligen Verarbeitungsvorgänge und der damit verbundenen Risiken

Mit der DSFA werden daher die Auswirkungen und Risiken der Verarbeitungsvorgänge für die Rechte und Freiheiten der Betroffenen analysiert und die Folgen der vorgesehenen Verarbeitungsvorgänge für den Datenschutz abgeschätzt und geeignete Abhilfemaßnahmen ergriffen. Die DSFA liefert somit einen Rahmen für die Identifizierung, die Beurteilung, die permanente Überwachung und demzufolge auch für die Verringerung der Risiken für die Freiheiten bzw. die Rechte natürlicher Personen. Die Risikoanalyse und die Ableitung geeigneter organisatorischer bzw. technischer Schutzfunktionen sind integraler Bestandteil einer DSFA. Die Ergebnisse einer DSFA sollen in die Planung sowie in die Umsetzung von Verarbeitungsvorgängen einfließen. Es muss daher ein Prozess festgelegt sein und angewendet werden, der sicherstellt, dass Kriterien für die Durchführung einer DSFA festgelegt sind und diese durchgeführt wird.

Ob die Voraussetzungen für die Durchführung einer Datenschutz-Folgenabschätzung vorliegen, obliegt der Beurteilung der oder des Verantwortlichen selbst. Hat die/der Verantwortliche eine(n) Datenschutzbeauftragte(n) bestellt, muss sie/er diese(n) bei der Durchführung der Datenschutz-Folgenabschätzung zu Rate ziehen.

Unabhängig vom gewählten Verfahren einer Risikoanalyse ist gem. Art. 35 EU-DSGVO iVm § 52 Datenschutzgesetz eine DSFA anhand allgemeiner Kriterien durchzuführen, da in den meisten Fällen zum Zeitpunkt der DSFA noch keine Verarbeitungsvorgänge umgesetzt sind. Insbesondere in den folgenden zwei Fällen ist eine solche Abschätzung neben der systematischen bzw. umfangreichen Überwachung öffentlich zugänglicher Bereiche für besonders risikoreiche Verarbeitungsvorgänge auszuführen. Das ist der Fall, wenn die Datenverarbeitung aufgrund der Art bzw. des Umfangs sowie wegen der Umstände oder wegen der Zwecke voraussichtlich ein hohes Risiko für die Rechte sowie für die Freiheiten natürlicher Personen ausmachen. Ein hohes Risiko ergibt sich vordergründig bei der Nutzung neuer Technologien sowie wegen der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung.

Die Datenschutz-Folgenabschätzung ersetzt in der EU-DSGVO die bisherigen Meldepflichten. Die Anforderungen zur Meldung von Verletzungen an die Datenschutzbehörde gemäß § 55 Datenschutzgesetz bleiben davon unberührt.

5.4.1.1 Kriterien für die Durchführung einer DSFA

Die DSGVO bestimmt, dass eine Datenschutz-Folgenabschätzung insbesondere dann zu erfolgen hat, wenn etwa neue Technologien verwendet werden oder aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Die Datenschutzbehörde (DSB) hat Verordnungen erlassen, nach denen entweder

- zwingend eine DSFA durchzuführen ist (sog. „black-list"): Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)
- oder keine DSFA durchgeführt werden muss (sog. „white-list): Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)

Die DSGVO führt selbst konkret folgende weitere beispielhafte Fälle an, in denen ein hohes Risiko besteht:

- systematische und umfassende Bewertung persönlicher Aspekte, die insbesondere die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interesse, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel natürlicher Personen betreffen, auf Basis automatisierter Verarbeitung: Hiermit sind vor allem Profiling-Maßnahmen angesprochen, die als Grundlage für Entscheidungen dienen, die Rechtswirkungen gegenüber natürlichen Personen entfalten oder diese in erheblicher Weise beeinträchtigen können, z.B. bei der Frage, ob einer natürlicher Person ein Kredit gewährt wird oder nicht,
- bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten,
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche: z.B. mittels Videoüberwachung.

Die „Artikel 29-Datenschutzgruppe" hat Leitlinien zur Datenschutz-Folgenabschätzung und zur Beantwortung der Frage, ob eine Verarbeitung im Sinne der DSGVO „wahrscheinlich ein hohes Risiko mit sich bringt" herausgegeben (Anmerkung: Die Artikel-29-Datenschutzgruppe wurde durch den Europäischen Datenschutzausschuss EDSA ersetzt, die Leitlinien wurden durch den EDS bestätigt). Entsprechend dieser Leitlinien ist unter „systematisch" zu verstehen:

- eine Verarbeitung findet im Rahmen eines Systems statt
- die Verarbeitung erfolgt organisiert und methodisch und ist vorab festgelegt.

Für die Auslegung des Begriffs „umfassend“ sind folgende Anhaltspunkte heranzuziehen:

- die Zahl der Betroffenen (entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe)
- die verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente
- die Dauer oder Dauerhaftigkeit der Datenverarbeitung
- das geografische Ausmaß der Datenverarbeitung

Unter „Überwachung“ ist nach den Leitlinien das Ziel zu verstehen, dass die betroffene Person beobachtet oder kontrolliert werden soll.

5.4.1.2 Durchführung der DSFA

> *Die DSFA muss zum frühestmöglichen Zeitpunkt bereits in der Entwicklungsphase der Verarbeitungstätigkeiten begonnen werden, selbst wenn einige der Verarbeitungsvorgänge noch nicht bekannt sind.*

Im Verlauf der Entwicklung kann es auch erforderlich werden, dass einzelne Schritte der Datenschutz-Folgenabschätzung wiederholt werden müssen, da die Schwere bzw. Eintrittswahrscheinlichkeit der Risiken, die die Verarbeitung mit sich bringen, unter Umständen durch die Wahl bestimmter technischer oder organisatorischer Maßnahmen beeinflusst werden.

Die Durchführung einer DSFA ist daher keine einmalige Aufgabe, sondern vielmehr ein kontinuierlicher Prozess. Für diesen Prozess ist kein dediziertes Verfahren zur Durchführung einer DSFA vorgeschrieben. Allerdings lässt sich eine DSFA wie in den folgenden Abbildungen dargestellt in vier Phasen anwenden:

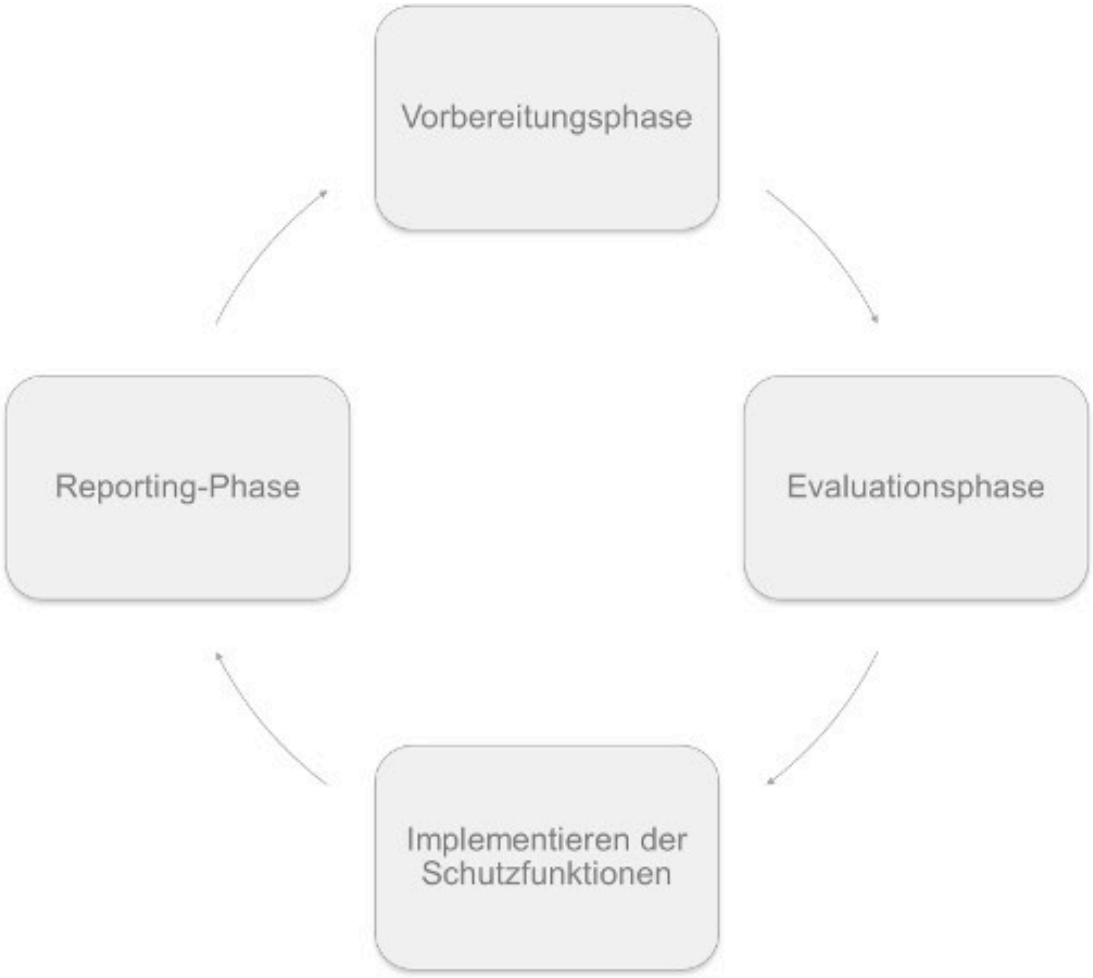

Abbildung 5.9: Die vier Phasen einer Datenschutz-Folgenabschätzung

Abbildung 5.10: Die Aktivitäten der jeweiligen Phase einer Datenschutz-Folgenabschätzung

Eine DSFA muss zumindest umfassen (vgl. DSGVO Art. 35 Abs 7):

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der/dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen;
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Bestimmungen der DSGVO eingehalten werden.

Die DSGVO lässt den für die Datenverarbeitung Verantwortlichen die nötige Flexibilität zur Festlegung der genauen Struktur und Form der DSFA, damit sie möglichst nahtlos in die bestehenden Arbeitsabläufe integriert werden kann. Auf Ebene der EU und auf internationaler Ebene wurde eine Vielzahl verschiedener Prozesse erarbeitet, die den in der DSGVO beschriebenen Komponenten Rechnung tragen. Unabhängig von ihrer Form muss es sich bei einer DSFA jedoch um eine

echte Risikoabschätzung handeln, auf deren Grundlage die für die Verarbeitung Verantwortlichen Abhilfemaßnahmen ergreifen können. Beispiele zu Methodiken für die DSFA sind im Anhang 1 der Leitlinien zur Datenschutz-Folgenabschätzung der „Artikel 29-Datenschutzgruppe“ zu finden.

Damit diese verschiedenen Ansätze parallel bestehen können und es den für die Verarbeitung Verantwortlichen dennoch möglich ist, der DSGVO zu entsprechen, wurden von der „Artikel 29-Datenschutzgruppe“ allgemeine Kriterien aufgestellt. Anhand dieser Kriterien lässt sich auch nachweisen, dass eine bestimmte DSFA-Methodik die Standards laut DSGVO-Anforderungen erfüllt.

Eine zulässige Datenschutz-Folgenabschätzung umfasst:

- eine systematische Beschreibung der Verarbeitungsvorgänge ist enthalten (vgl. DSGVO Artikel 35 Absatz 7 Buchstabe a):
    - die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sind berücksichtigt (vgl. DSGVO Erwägungsgrund 90);
    - die personenbezogenen Daten, die Empfänger und die Speicherfrist für die personenbezogenen Daten sind festgehalten;
    - eine funktionale Beschreibung der Verarbeitungsvorgänge ist enthalten;
    - die Wirtschaftsgüter, auf die sich die personenbezogenen Daten stützen (Hardware, Software, Netzwerke, Personen, Papiere oder Übertragungsmedien für Papiere), wurden ermittelt;
    - die Einhaltung genehmigter Verhaltensregeln ist berücksichtigt (vgl. DSGVO Artikel 35 Absatz 8);
- die Notwendigkeit und Verhältnismäßigkeit wurden bewertet (vgl. DSGVO Artikel 35 Absatz 7 Buchstabe b):
    - Maßnahmen zur Einhaltung der Verordnung wurden bestimmt (vgl. DSGVO Artikel 35 Absatz 7 Buchstabe d und Erwägungsgrund 90), wobei Folgendes berücksichtigt wurde:
        - Maßnahmen im Sinne der Verhältnismäßigkeit und Notwendigkeit der Verarbeitung, und zwar auf folgender Grundlage:
            - festgelegte, eindeutige und legitime Zwecke (vgl. DSGVO Artikel 5 Absatz 1 Buchstabe b);
            - Rechtmäßigkeit der Verarbeitung (vgl. DSGVO Artikel 6);
            - Daten, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind (vgl. DSGVO Artikel 5 Absatz 1 Buchstabe c);
            - begrenzte Speicherfrist (vgl. DSGVO Artikel 5 Absatz 1 Buchstabe e);
        - Maßnahmen im Sinne der Rechte der Betroffenen:

- Informationspflicht gegenüber den Betroffenen (vgl. DSGVO Artikel 12, 13 und 14);
- Auskunftsrecht und Recht auf Datenübertragbarkeit (vgl. DSGVO Artikel 15 und 20);
- Recht auf Berichtigung und Löschung (vgl. DSGVO Artikel 16, 17 und 19);
- Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (vgl. DSGVO Artikel 18, 19 und 21);
- Verhältnis zu Auftragsverarbeitern (vgl. DSGVO Artikel 28);
- Garantien in Bezug auf die internationale Übermittlung von Daten (vgl. DSGVO Kapitel V);
- vorherige Konsultation (vgl. DSGVO Artikel 36).

- die Risiken für die Rechte und Freiheiten der betroffenen Personen werden kontrolliert (vgl. DSGVO Artikel 35 Absatz 7 Buchstabe c):
  - Ursache, Art, Besonderheit und Schwere der Risiken (vgl. DSGVO Erwägungsgrund 84) wurden aus Sicht der Betroffenen bewertet, und zwar genau genommen für jedes einzelne Risiko (unrechtmäßiger Datenzugriff, unerwünschte Änderung und Verschwinden von Daten):
    - Risikoquellen wurden berücksichtigt (vgl. DSGVO Erwägungsgrund 90);
    - potenzielle Auswirkungen auf die Rechte und Freiheiten von Betroffenen wurden ermittelt, die bei Ereignissen wie z. B. einem unrechtmäßigen Datenzugriff, einer unerwünschten Änderung und dem Verschwinden von Daten bestehen könnten;
    - Bedrohungen wurden ermittelt, die einen unrechtmäßigen Datenzugriff, eine unerwünschte Änderung und das Verschwinden von Daten nach sich ziehen könnten;
    - Eintrittswahrscheinlichkeit und Schwere wurden bewertet (vgl. DSGVO Erwägungsgrund 90);
  - Maßnahmen zur Bewältigung dieser Risiken wurden ermittelt (vgl. DSGVO Artikel 35 Absatz 7 Buchstabe d und Erwägungsgrund 90);
- betroffene Parteien wurden einbezogen:
  - der Rat des Datenschutzbeauftragten wurde eingeholt (vgl. DSGVO Artikel 35 Absatz 2);
  - gegebenenfalls wurde der Standpunkt der betroffenen Personen oder ihrer Vertreter eingeholt (vgl. DSGVO Artikel 35 Absatz 9).

5.4.1.3 Konsultation der Datenschutzbehörde

Sollte auf Basis der Datenschutz-Folgenabschätzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person festgestellt werden und kann die/der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos treffen, muss sie/er vor der Verarbeitung die Datenschutzbehörde (DSB) konsultieren.

Die DSB kann der/dem Verantwortlichen und gegebenenfalls dem/der Auftragsverarbeiter/in innerhalb eines Zeitraumes von bis zu 8 Wochen nach Erhalt des Konsultationsersuchens schriftliche Empfehlungen erteilen. Sollte der beabsichtigte Datenverarbeitungsvorgang eine entsprechende Komplexität aufweisen, kann diese Frist um 6 Wochen verlängert werden. Die/der Verantwortliche oder gegebenenfalls der/die Auftragsverarbeiter/in sind über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Konsultationsersuchens von der Datenschutzbehörde zu informieren.

5.4.2 Risikomanagement im Kontext der NIS2-Richtlinie

Die NIS2-Richtlinie (RICHTLINIE (EU) 2022/2555 vom 14.12.2022) soll ein hohes Maß an Cybersicherheit in der EU ermöglichen und legt daher einen Europäischen Rahmen für die Realisierung von Rechtssicherheit hinsichtlich Risikomanagement im Bereich der Cybersicherheit fest und stärkt die damit verbundenen Berichtspflichten. Damit soll verhindert werden, dass Cyberbedrohungen in Sicherheitsvorfälle übergehen, die erhebliche materielle oder immaterielle Schäden verursachen. Ein geeignetes Risikomanagement wird einerseits für die vom Anwendungsbereich betroffenen Einrichtungen (d.h. wesentliche Einrichtungen und wichtige Einrichtungen sowie digitale Infrastruktur) der NIS2-Richtlinie gefordert aber andererseits sollen die Mitgliedsstaaten bestrebt sein, dass nach Erwägungsgrund (13) NIS2-RL selbst Einrichtungen die von der NIS2-RL ausgenommen sind, ein hohes Maß an Cybersicherheit erreichen.

Im Anwendungsbereich der NIS2-RL befinden sich sowohl Großunternehmen als auch mittlere Unternehmen. Demzufolge soll die Umsetzung zumindest gleichwertiger Maßnahmen für den Bereich des Risikomanagements für solche Einrichtungen zum Risikomanagement im Bereich der Cybersicherheit forciert werden. Das bedeutet, die NIS2-RL definiert ein zumindest anwendbares Grundniveau für Risikomanagementmaßnahmen und damit verbundene Berichtspflichten im Bereich der Cybersicherheit für die in den Anwendungsbereich der Richtlinie fallenden Sektoren bzw. die darunter eingeordneten Einrichtungen. Zusätzlich können etwa sektorspezifische Rechtsakte wie beispielsweise ein solcher Durchführungsrechtsakt folgen.

Bei der Auswahl und der Festlegung von Risikomanagementmaßnahmen soll im Rahmen der NIS2-RL die Risikoexposition und eine damit verbundene Kritikalität der betroffenen Einrichtungen in geeigneter Form für wesentliche Einrichtungen einerseits sowie für wichtige Einrichtungen und die digitale Infrastruktur andererseits berücksichtigt werden. Das gilt sowohl für den Fall, dass die betroffenen Einrichtungen den Betrieb bzw. deren Wartung eigenständig d.h. intern bewerkstelligen oder für den Fall, dass diese Einrichtungen Aufgaben ferner an Dienstleisterinnen bzw. Dienstleister auslagern.

Für weitere generelle Informationen zum Thema NIS sei auf das Kapitel 16.2 Sicherheit von Netz- und Informationssystemen (NIS) verwiesen.

5.4.2.1 Anwendungsbereich der NIS2-RL

Anwendbar ist die NIS2-RL für sogenannte kritische Sektoren oder für betroffene Einrichtungen. Es lassen sich zwei verschiedene Arten solcher Sektoren unterscheiden: (1) Besonders kritische Sektoren (für „wesentliche Einrichtungen“) und (2) Weitere kritische Sektoren (für „Wichtige Einrichtungen“). Einerseits lassen sich generell wesentliche Einrichtungen als solche einordnen, insofern diese bei Verlust bzw. Ausfall oder Unterbrechung derer Dienste schwerwiegende Auswirkungen auf das Gesundheitswesen, oder die Wirtschaft, Energieversorgung, Kommunikation sowie auf die öffentliche Verwaltung hervorgerufen werden.

Wesentliche Einrichtungen für besonders kritische Sektoren

- Energie (Elektrizität/Strom, Fernwärme, -kälte, Gas, Öl, Wasserstoff)
- Verkehr (Luft, Schiene, Straße, Wasser)
- Bankwesen (z.B. Hausbanken, Kreditinstitute)
- Finanzmarktinfrastrukturen (Central Clearing Counterparties - CCPs, Central Security Depositories – CDSs sog. „Zentralverwahrer“)
- Gesundheitswesen (inkl. Herstellung von Impfstoffen bzw. pharmazeutischen Produkten)
- Trinkwasser
- Abwasser
- Digitale Infrastrukturen (z.B. Internet-Exchange-Ports, DNS, Cloud-Computing-Dienste, Rechenzentrumsdienste, Netzwerke, Vertrauensdiensteanbieter, öffentlich zugängliche Kommunikationsnetze bzw. -dienste)
- IKT-Dienstleistungsmanagement (z.B. Business-to-Business – B2B)
- Öffentliche Verwaltung
- Weltraum

Wichtige Einrichtungen für weitere kritische Sektoren

- Post- und Kurierdienste bzw. Lieferdienste
- Abfallwirtschaft
- Chemikalien (Herstellung, Produktion und Vertrieb)
- Lebensmittel (Produktion, Verarbeitung, Vertrieb)
- Fertigung (z.B. medizinische Geräte, Elektrogeräte, Computer etc.)
- Digitale Dienste (z.B. Online-Marktplätze, Online-Suchmaschinen)

Die Umsetzung eines ISO 27001-konformen ISMS kann muss aber nicht ausreichend sein, um die Anforderungen der NIS2-RL zu erfüllen.

5.4.2.2 Pflichten aus der NIS2-RL

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen sowie für die digitale Infrastruktur die sich im Anwendungsbereich der NIS2-RL befinden, sind für die Einhaltung der im Artikel 21 der NIS2-RL festgelegten Maßnahmen für ein geeignetes Risikomanagement verantwortlich. Daraus ergibt sich auch die Pflicht zur Überwachung der ausgewählten und umgesetzten Risikomanagementmaßnahmen.

Schulungen

Darüber hinaus muss das Leitungspersonal wesentlicher und wichtiger Einrichtungen selbst an Schulungen teilnehmen. Auch muss die Leitung den Mitarbeiterinnen und Mitarbeitern regelmäßig Schulungen ermöglichen, um die Kenntnisse bzw. Fähigkeiten zu erwerben, Risiken im Zusammenhang mit den erbrachten Diensten zu erkennen und diese zu bewerten. Zu diesem Zweck sollen die Schulungen zumindest die folgenden sieben Themenfelder abdecken:

1. Risikomanagement
2. Cybersicherheit
3. IT-Sicherheit
4. Informationssicherheit
5. Netzwerksicherheit
6. Security Awareness
7. Managementpraktiken in den zuvor genannten Themenfeldern

Durch die Teilnahme an solchen Schulungen sollen ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken für die betroffenen Dienste ermöglicht werden. Auch sollen relevante Managementpraktiken vermittelt werden und die Auswahl geeigneter Maßnahmen zur Behandlung der Risiken unterstützt werden.

Diese Schulungen haben nicht den Zweck, die Leitungsebene zu Cybersecurity-Expertinnen oder Experten auszubilden. Da die Leitung aber für die Planung und die Organisation der Maßnahmen zum Risikomanagement verantwortlich ist, ist ein Grundverständnis, das in diesen Schulungen regelmäßig vermittelt werden soll, als Voraussetzung zur Umsetzung solcher Maßnahmen zu verstehen.

Umsetzungsverantwortung der Leitung

Die Leitung einer Einrichtung muss nicht jede Aufgabe selbst erledigen.
Das bedeutet, die Leitung einer Einrichtung muss die Planung für Risikomanagementmaßnahmen entweder durchführen oder durchführen lassen. Zudem ist ein organisatorischer Rahmen durch die Leitung zu schaffen und es sind die Rahmenbedingungen zu etablieren, damit in der Organisation ein generelles Verständnis für Cybersicherheit vorhanden ist. Anschließend muss die Umsetzung der Risikomanagementmaßnahmen sichergestellt sein.

Die realisierten Maßnahmen müssen in einem nächsten Schritt kontinuierlich geprüft und evaluiert werden. Auch muss die Leitung dafür sorgen, dass regelmäßige Risikoanalysen durchgeführt werden, um die Gefahrensituation zu prüfen und notwendige Verbesserungen zu initiieren und umzusetzen. Schlussendlich soll die laufende Überprüfung dazu führen, dass die Maßnahmen aber auch der organisatorische Rahmen kontinuierlich verbessert wird und diese Verbesserungen im Gleichklang mit dem Risikoprofil der Einrichtung umgesetzt werden.

5.4.2.3 Risikomanagement-Maßnahmen

Die auszuwählenden und umzusetzenden Maßnahmen für das Risikomanagement im Rahmen der NIS2-RL sind unter Berücksichtigung der folgenden vier Eckpunkte zu realisieren:

- Stand der Technik
- Unter Berücksichtigung einschlägiger europäischer und internationalen Normen
- Kosten für die Umsetzung
- Erreichen eines Sicherheitsniveaus, das dem vorhandenen Risiko (z.B. Risikoprofil) angemessen ist

Zur Auswahl der Maßnahmen für das Risikomanagement sind sowohl das Risikoprofil bzw. die Risikoexposition als auch Restrisiken zu berücksichtigen.
Das bedingt ferner, dass sowohl die Wahrscheinlichkeit für einen Eintritt eines Sicherheitsvorfalls („Incident“) neben der Schwere und den damit verbundenen Auswirkungen eines eingetretenen Sicherheitsvorfalls ebenso zu berücksichtigen ist. Das bedeutet die Materialisierung eines Schadens der durch ein eingetretenes Schadensereignis hervorgerufen wird, ist zu berücksichtigen. Insbesondere müssen die Auswirkungen eines eingetretenen Sicherheitsvorfalls im Hinblick auf gesellschaftliche und auf wirtschaftliche Auswirkungen in die Bewertung einfließen.

Die konsolidierten 10 Risikomanagement-Maßnahmen im Bereich der Cybersicherheit nach der Art. 21 der NIS2-Richtlinie sind:

- Konzept zur Risikoanalyse für die risikobasierte Sicherheit von Informationssystemen
- Verfahren und Abläufe für die Bewältigung von Sicherheitsvorfällen („Incidents“)
- Business Continuity Management, Notfallmanagement sowie Krisenmanagement und Wiederanlaufpläne
- Lieferkettensicherheit („Supply Chain Security“) zum Management von Beziehungen zwischen Einrichtungen und etwa deren Zulieferbetrieben bzw. Kundinnen/Kunden
- Sicherheit im Lebenszyklus von IKT-Systemen (z.B. Erwerb, Entwicklung, Betrieb bzw. Wartung)
- Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- Verfahren zur Cyberhygiene und für Schulungen zur Cybersicherheit („Awareness“)
- Konzepte und Verfahren für die Verwendung kryptografischer Verfahren und insbesondere ggfs. Nutzung von Verschlüsselung
- Maßnahmen zur Personalsicherheit und Konzepte bzw. Verfahren für die Zugriffskontrolle (z.B. auf Daten, Räumlichkeiten, Speichermedien)
- Absicherung mittels Multifaktorauthentifizierung oder kontinuierlicher Authentifizierung und ergänzend abgesicherte Kommunikationsverbindungen (z.B. Video, Sprache, Textnachrichten) und geschützte Notfallkommunikationssysteme

Für eine geeignete Auswahl der oben beschriebenen Maßnahmen zum Risikomanagement sind der aktuelle Stand der Technik sowie relevante Normen zur Informationssicherheit bzw. zur IT- oder zur Cybersicherheit bzw. internationale Best Practices zur Bewertung heranzuziehen. Die Auswahl solcher Risikomanagement-Maßnahmen und deren Kombination muss dem Risikoprofil der Einrichtung entsprechen sowie die akzeptierten Restrisiken berücksichtigen. Auch ist es möglich die Kosten zur Realisierung von Risikomanagement-Maßnahmen bei der Auswahl in Erwägung zu ziehen und den sogenannten Risikokosten gegenüberzustellen, um die Auswahl der Maßnahmen zu erleichtern oder diese in geeigneter Form fundiert zu begründen.

Die NIS2 legt einen Schwerpunkt auf das Risikomanagement, insbesondere in betroffenen Einrichtungen, und verpflichtet diese, mögliche Risiken für die Cybersicherheit im Unternehmen vorab zu identifizieren und diese systematisch zu bewerten, um schließlich darauf aufbauend geeignete Gegenmaßnahmen zu realisieren. Die NIS2-RL umfasst auch Anforderungen zu Berichtspflichten nämlich

an die Meldung von Sicherheitsvorfällen sowie Anforderungen an die systematische Behandlung solcher Vorfälle, damit einerseits Cyberangriffe weniger wahrscheinlich werden und falls ein solcher Cyberangriff schlussendlich doch eintritt, dessen Auswirkungen reduziert werden können.

6 Organisation

6.1 Interne Organisation

In der Folge werden zunächst die Grundsätze und Maßnahmen des Informationssicherheitsmanagements innerhalb der Organisation dargestellt. Voraussetzung dafür ist eine aktive Rolle der Managementebene bei der Implementierung, Kontrolle und Weiterentwicklung der Informationssicherheitsmaßnahmen sowie der Etablierung und Pflege von Kontakten zu Behörden, Institutionen, Sicherheitsexperten und Interessensgruppen.

- Die Managementebene wird über mögliche Risiken und Konsequenzen aufgrund mangelhafter Informationssicherheit informiert.
- Sie übernimmt die Gesamtverantwortung für Informationssicherheit.
- Sie initiiert und steuert den Informationssicherheitsprozess innerhalb der Organisation.
- Sie delegiert einzelne Aufgaben im Bereich der Informationssicherheit an den verantwortlichen Beauftragten für Informationssicherheit (zumeist bezeichnet als CISO – Chief Information Security Officer; früher auch bezeichnet als IT-Sicherheitsbeauftragter).

6.1.1 Managementverantwortung

Die oberste Managementebene jeder Behörde, jeder Institution und jedes Unternehmens ist dafür verantwortlich, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken frühzeitig erkannt und minimiert werden. Dies kann auch, je nach Organisationsform und Geschäftsbereich, in verschiedenen Regelwerken festgelegt sein. Mit der steigenden Abhängigkeit der Geschäftsprozesse von der Informationstechnik steigen auch die Anforderungen, dass die Informationssicherheit nach innen und außen gewährleistet ist.

In welchem Ausmaß Informationssicherheit erreicht und erhalten wird, hängt weitgehend vom Engagement und der Unterstützung des Managements ab. Abgesehen von der Bereitstellung dafür notwendiger finanzieller und personeller Ressourcen müssen klare Ziele und Richtlinien vorgegeben und die jeweiligen Rollen sowie damit verbundene Verantwortlichkeiten festgesetzt werden. Letztlich kommt es aber auch darauf an, dass insbesondere die Managementebene die Sicherheitsmaßnahmen auch selbst vorbildlich lebt.

Dazu hat die Managementebene die Aufgabe, Folgendes zu veranlassen:

- Ermitteln der Sicherheitsrisiken für die Organisation und die Informationen sowie damit verbundene Auswirkungen und Kosten.
- Darstellung der Auswirkungen von Sicherheitsvorfällen auf kritische Geschäftsprozesse.
- Darstellung der Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben.
- Identifikation von Informationssicherheits-Zielen und festlegen des organisatorischen bzw. technischen Geltungsbereichs (sog. Informationsverbund).
- Erarbeitung, Überprüfung und Genehmigung der Informationssicherheitspolitik.
- Planen und einrichten einer Informationssicherheitsorganisation.
- Integration der Maßnahmen in die Prozesse der Organisation.
- Etablierung von Mechanismen, um die Wirksamkeit der Maßnahmen der Informationssicherheitspolitik zu überprüfen.
- Etablierung von Mechanismen, um das Informationssicherheits-Niveau aufrecht zu erhalten.

Die Managementebene muss allerdings die Informationssicherheitsziele so definieren, dass sie in allen Bereichen mit den verfügbaren Ressourcen (Personal, Zeit, Finanzmittel) erreichbar sind.

Hilfestellungen kann die Managementebene dabei von branchentypischen Standard-Vorgehensweisen zur Informationssicherheit, von InformationssicherheitsexpertInnen der eigenen Organisation und externen BeraterInnen erhalten.

[Quelle: BSI-Standard 200-2]

6.1.1.1 Zusammenwirken verantwortliches Management - MitarbeiterInnen - Gremien

Die Managementebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Verantwortung für Informationssicherheit verbleibt auch dort, die Aufgabe „Informationssicherheit“ wird allerdings typischerweise an eine/n Beauftragte/n zur Informationssicherheit sog. Chief Information Security Officer (CISO) delegiert. Dabei ist eine intensive Beteiligung der Führungsebene im „Managementprozess Informationssicherheit“ erforderlich.

Nur so kann das Informationssicherheitsmanagement sicherstellen, dass keine untragbaren Risiken bestehen und Ressourcen an der richtigen Stelle investiert werden. Die oberste Managementebene ist somit diejenige Instanz, die die Entscheidung über den Umgang mit Risiken trifft, auftretenden Restrisiken zustimmt und die entsprechenden Ressourcen zur Verfügung stellen muss.

Die Managementebene trägt die Verantwortung zur Prävention und Behandlung von Sicherheitsrisiken. Dementsprechend sind die Zuständigkeiten und Verantwortlichkeiten bezüglich Informationssicherheitsthemen zu klären. Allerdings wird rechtzeitige Information über mögliche Risiken beim Umgang mit Informationen, Geschäftsprozessen und IT von der Managementebene häufig als Bringschuld der IT- oder Sicherheitsexperten gesehen, speziell wenn es bereits zu einem Sicherheitsvorfall gekommen ist. Daher sollten diese die Managementebene über mögliche Risiken und Konsequenzen aufgrund mangelhafter Informationssicherheit regelmäßig informieren. Dies enthebt die Managementebene jedoch nicht von ihrer Verantwortung, dass sie von solchen Informationen umfassend und rechtzeitig erreicht wird.

Abhängig von Größe und Struktur der Organisation kann dies durch bestehende oder speziell eingerichtete Managementorgane oder -gremien umgesetzt werden.

Die Leitungsebene trägt zwar die Verantwortung für die Erreichung der Sicherheitsziele, der Sicherheitsprozess muss aber von allen Beschäftigten in einer Organisation mitgetragen und mitgestaltet werden. Idealerweise sollten dabei folgende Prinzipien eingehalten werden:

- Die Initiative für Informationssicherheit geht von der Managementebene aus.
- Die Gesamtverantwortung für Informationssicherheit verbleibt bei der obersten Managementebene.
- Die Aufgabe „Informationssicherheit“ wird durch die Managementebene aktiv unterstützt.
- Die Managementebene benennt die für Informationssicherheit zuständigen MitarbeiterInnen und stattet diese mit den erforderlichen Kompetenzen und Ressourcen aus.
- Die Managementebene übernimmt auch im Bereich Informationssicherheit eine Vorbildfunktion, vor allem indem sie selbst die vorgegebenen Sicherheitsregeln beachtet.

Die Managementebene muss sich dafür einsetzen, dass Informationssicherheit in alle relevanten Geschäftsprozesse bzw. Fachverfahren und Projekte integriert wird und, dass die Angemessenheit und Wirksamkeit aller Elemente des Sicherheitsmanagements ständig überprüft und verbessert werden. Der/Die CISO braucht hierbei erfahrungsgemäß die volle Unterstützung der Managementebene, um unter dem überall herrschenden Erfolgsdruck von den jeweiligen Fachverantwortlichen in jede wesentliche Aktivität eingebunden zu werden.

[Quelle: BSI-Standard 200-2]

6.1.2 Koordination

Um das angestrebte Sicherheitsniveau zu erreichen, muss die Informationssicherheitsorganisation in Verbindung mit einem Informationssicherheitsprozess organisationsweit umgesetzt werden. Dazu sind Rollen innerhalb der Organisation festzulegen und diesen entsprechende Aufgaben zuzuordnen. Diese Rollen werden dann qualifizierten MitarbeiterInnen zur Ausführung übertragen. Damit können alle wichtigen Aspekte berücksichtigt und die Aufgaben effizient und effektiv erledigt werden.

Meistens umfasst die Koordination der Informationssicherheit die Zusammenarbeit von ManagerInnen, AdministratorInnen, BenutzerInnen, EntwicklerInnen sowie AuditorInnen und Sicherheitspersonal. Wenn nötig sollten auch FachexpertInnen (Recht, Risikomanagement, Personalwesen) eingebunden werden. Aktivitäten im Rahmen einer solchen Zusammenarbeit sind:

- Abgleichen der Sicherheitsaktivitäten mit der Informationssicherheitspolitik.
- Maßnahmen, wenn kein Einklang mit der Informationssicherheitspolitik herstellbar ist.
- Abstimmung und Beschlusslagen für die erforderlichen Maßnahmen.
- Identifikation von bestehenden oder sich verändernden Bedrohungen, denen die Informationen und informationsverarbeitenden Einrichtungen ausgesetzt sind.
- Bewertung der Eignung und Wirksamkeit der Sicherheitsmaßnahmen.
- Schaffung und Förderung von Awareness und Etablierung von Ausbildungs- und Schulungsmaßnahmen für Informationssicherheit.
- Schlussfolgerungen und Verbesserungsmaßnahmen aus Informationssicherheits-Vorfällen (in der eigenen oder auch anderen Organisationen)

Wie viele und welche Personen mit Informationssicherheit befasst sind, hängt selbstverständlich von der Größe, Beschaffenheit und Struktur der jeweiligen Organisation ab. Zumindest sollte es jedoch eine/einen Sicherheitsbeauftragten als zentralen AnsprechpartnerIn für die Koordination des Informationssicherheitsprozesses geben.

Gibt es - etwa in größeren Organisationen - mehrere befasste Personen, kann ein IS-Management-Team aufgebaut werden. Es regelt die übergreifenden Belange der Informationssicherheit und arbeitet Pläne, Vorgaben und Richtlinien aus. Um den direkten Zugang zur obersten Managementebene sicherzustellen, sollten diese Rollen als Stabsstelle organisiert sein. Der/Die CISO soll direkt einem/einer für Informationssicherheit verantwortlichen ManagerIn berichten.

Unbeschadet davon sind alle MitarbeiterInnen für die Aufrechterhaltung der Informationssicherheit an ihrem Arbeitsplatz und in ihrer Umgebung verantwortlich.

Siehe dazu auch 6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit.

[Quelle: BSI-Standard 200-2]

6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit

Um eine Berücksichtigung aller wichtigen Aspekte und eine effiziente Erledigung sämtlicher anfallender Aufgaben zu gewährleisten, ist es erforderlich, die Rollen und Verantwortlichkeiten aller in den Informationssicherheitsprozess involvierten Personen klar zu definieren.

Die Organisation des ISM ist für jede Institution - entsprechend ihrer Größe, Struktur und Aufgaben - spezifisch festzulegen und in der Informationssicherheitspolitik festzuschreiben.

Zentrale Aufgaben im Informationssicherheitsmanagementprozess übernehmen dabei

- der/die CISO (zur Wahl der Bezeichnung s. u.)
- der/die StellvertreterIn der/des CISO
- das Informationssicherheitsmanagement-Team
- der/die Informationssicherheitskoordinator/in (z.B. eines Bereiches)
- die Applikations-/Projektverantwortlichen.

Auf der Ebene der Bundesverwaltung ist zusätzlich in jedem Ressort die Person einer/eines Informationssicherheitsbeauftragten gemäß Informationssicherheitsgesetz (InfoSiG) einzurichten. Weiters werden für diesen Bereich durch das IKT-Board verbindliche Regelungen zur IKT-Sicherheit vorgegeben.

Es ist zu betonen, dass es sich bei diesen Funktionen bzw. Gremien, die im Folgenden näher beschrieben werden, um Rollen handelt, die - abhängig von der Größe und den Sicherheitsanforderungen einer Organisation - durchaus auch von mehreren Personen wahrgenommen werden können. In diesem Fall ist auf eine genaue Trennung der Kompetenzen und Verantwortlichkeiten Bedacht zu nehmen. Genauso ist es möglich, dass eine Person eine dieser Rollen zusätzlich zu anderen Aufgaben übernimmt. So könnte beispielsweise SystemadministratorInnen als Informationssicherheitskoordinator/in des jeweiligen Fachbereichs für dieses System agieren. Dabei ist aber unbedingt darauf zu achten, dass ausreichend Zeit für die sicherheitsrelevanten Tätigkeiten zur Verfügung steht und es zu keinen Kollisionen von Verantwortlichkeiten oder Interessen kommt.

Nachfolgend werden die wichtigsten typischen Aufgaben und Verantwortlichkeiten dieser Funktionen bzw. Gremien kurz beschrieben. Eine detaillierte, auf die speziellen Aufgaben und Anforderungen der betreffenden Organisation abgestimmte Beschreibung ist im Rahmen der organisationsweiten Informationssicherheitspolitik zu geben.

6.1.3.1 Die/Der CISO

Die/Der CISO ist als Manager (idealerweise der höheren Managementebene) für die Informationssicherheit in Behörden, Institutionen, Ressorts bzw. Unternehmen ("Organisationen") oder Teilen davon sowie für deren strategischen Aufbau und kontinuierlichen Ausbau verantwortlich. Zu diesem Zweck ist die/der CISO zentrale Ansprechperson für alle Informations- und IT-Sicherheitsfragen innerhalb einer Organisation sowie bei organisationsübergreifenden Interessensgruppen oder Gremien im Bereich der Informations- und IT-Sicherheit und trägt die fachliche Verantwortung für diesen Bereich. Eine direkte Berichtslinie an das Top Level Management wird explizit empfohlen, ist jedoch nicht in allen Fällen eine notwendige Voraussetzung.

Anmerkung: Die Bezeichnung „CISO" für die Person einer/eines zentralen Sicherheitsverantwortlichen wurde zum einen gewählt, weil es sich um einen in vielen Institutionen sowohl des Behörden- als auch des Privatwirtschaftsbereiches eingeführten Begriff handelt, zum anderen, um diese Rolle gegenüber der Rolle der/des Informationssicherheitsbeauftragten gemäß Informationssicherheitsgesetz (InfoSiG) abzugrenzen, der/dem ganz spezifische Aufgaben lt. Gesetz zukommen. Bei einer alternativ bzw. ehemals verwendeten Bezeichnungen handelt es sich etwa um den/die Informationssicherheitsmanager/in.

Der/die CISO soll möglichst unabhängig agieren können, aber dennoch in enger Kooperation mit dem Tagesgeschäft bzw. mit den Kernprozessen sowie mit den Unterstützungsprozessen und mit der IT verbunden sein.

Einerseits unterstützt der/die CISO die Managementebene, um die Einhaltung rechtlicher, regulativer und vertraglicher Verpflichtungen, die durch ein Kompromittieren der Informationssicherheit gefährdet sind, zu ermöglichen. Andererseits wird der/die CISO bei der Umsetzung der übertragenen Aufgaben durch eine Informationssicherheitsorganisation unterstützt (z.B. definiert in einer Informationssicherheitsleitlinie). Demzufolge muss der/die CISO das Sicherheitsmanagement zusätzlich im Rahmen der definierten Pflichten kontinuierlich steuern sowie nachvollziehbar gestalten.

Zu den Pflichten der/des CISO gehören:

- Das Informationssicherheitsmanagement und den damit verbundenen Informationssicherheitsprozess operativ einzurichten, zu steuern und zu koordinieren sowie kontinuierlich zu verbessern
- die verantwortliche Mitwirkung an der Erstellung des Informationssicherheitsprozesses (bzw. Informationssicherheitskonzepts) und des Informationssicherheitsrisikomanagements sowie weitere Richtlinien und Regelungen zur Informationssicherheit (z.B. Informationssicherheitsrichtlinien, Sicherheitskonzept, Notfallvorsorgekonzept, …)
- Umsetzen der Informationssicherheitspolitik

- Veranlassen der Erstellung einer konsolidierten Übersicht vorhandener Assets durch Identifikation von Anwendungen, IT-Systemen und Netzwerkkomponenten auf der Grundlage wesentlicher Geschäftsprozesse bzw. Fachverfahren unter Berücksichtigung direkt erforderlicher Abhängigkeiten sowie kritischer Unterstützungsprozesse
- Veranlassen und Mitwirken an der Erstellung von Informationssicherheitsrisikoanalysen und Bewertung der identifizierten Risiken
- die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen
- Untersuchen bzw. managen von Sicherheitsvorfällen (z.B. Cybervorfälle, Cyberkrisen)
- die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen in Bezug auf Informationssicherheit
- die Gewährleistung der Informationssicherheit im laufenden Betrieb
- die Verwaltung der für Informationssicherheit zur Verfügung stehenden Ressourcen sowie
- gemeinsame Abstimmung und agieren als zentrale Ansprechstelle in Belangen der Informationssicherheit zur internen Koordination (z.B. Datenschutzbeauftragte/r) sowie bei organisationsübergreifenden Interessensgruppen oder Gremien.

Der Funktion der/des CISO kommt eine zentrale Bedeutung zu. Daher sollte diese Rolle in jedem Fall - also auch bei kleinen Organisationen - definiert und klar einer Person, eventuell zusätzlich zu anderen Aufgaben, zugeordnet sein. Demzufolge muss die Effektivität der Rolle des/der CISO durch eine geeignete Auswahl qualifizierten Personals sichergestellt sein und es ist eine zweckmäßige Positionierung innerhalb der eigenen Organisations- bzw. Entscheidungsstrukturen sicherzustellen. Eine Möglichkeit wäre zum Beispiel die Etablierung als Stabstelle.

Das Anforderungsprofil an einen CISO umfasst zumindest:

- **Qualifikation im Bereich Informationssicherheitmanagement:** Geeignete Kenntnisse des Informationssicherheitsmanagements (z.B. ISO2700x, IT-Grundschutz) als auch im zugrundeliegenden Risikomanagement (z.B. ISO/IEC 31000, BSI 200-3) sind notwendige Voraussetzungen. Dies fordert Fachwissen über relevante Zusammenhänge zwischen Sicherheits-, Kontinuitäts-, Risiko- und Compliancemanagement sowie der IT, aber auch über Prozesse, die Ressourcen und zur Organisation. Darüber hinaus muss die/der CISO in der Lage sein, bei Sicherheitsvorfällen (z.B. Cybervorfällen und in Cyberkrisen) als Teil des Krisenmanagements zu agieren bzw. als Ansprechpartner (z.B. für die gemäß Cyberkrisenmanagement – CKM etablierten Einsatzstrukturen) zu agieren. Die/Der CISO koordiniert und verantwortet die Erhebung, Analyse und Bewertung von Risiken für die Informationssicherheit der Organisation. Darüber hinaus wird Domänenwissen in rechtlicher und regulatorischer Hinsicht gefordert.

- **Qualifikation im Bereich Informationstechnologie:** Grundlegendes Verständnis für die IT-Systeme und damit verbundene Abhängigkeiten der eigenen Organisation, sowie für IT-Absicherungskonzepte, vor allem in Hinblick auf für die Informationssicherheit relevante Aspekte. Die/Der CISO ist in der Lage, ihr/ihm aufbereitete technische Konzepte der strategischen Führungsebene darzustellen und dort Entscheidungen zu erwirken.
- **Kommunikationsfähigkeiten:** Hohes Maß an Kommunikationsfähigkeit und die Befähigung sowohl mit Technikern als auch Entscheidungsträgern der strategischen Ebene kommunizieren zu können. Da die/der CISO in einer Querschnittsmaterie arbeitet, haben Maßnahmen in ihrem/seinem Verantwortungsbereich zumeist Auswirkungen auf unterschiedliche Elemente der Linienorganisation (z.B. Aufbau- bzw. Ablauforganisation). Demzufolge wird von der/dem CISO gleichzeitig ein hohes Maß an Diplomatie als auch Durchsetzungskraft gefordert. Die/Der CISO muss darüber hinaus jederzeit direkten Zugang zur strategischen Entscheidungsebene haben.
- **Kooperation mit anderen Beteiligten:** Beim Management der Informationssicherheit und damit verbundener Informationssicherheitsrisiken sind Schnittstellen zu angrenzenden (sich ergänzenden) Fachgebieten (z.B. Datenschutz, Risikomanagement) bzw. Organisationen (z.B. Aufsicht, Kooperationspartner, Zulieferbetriebe) zu berücksichtigen. Der/Die CISO muss diese Schnittstellen aktiv fördern und Grundlegendes Fachwissen über die angrenzenden Fachgebiete aufweisen, um die übergreifende Kommunikation bzw. Kooperation (z.B. Austausch über relevante Risiken) zu realisieren.

Fachliche Anforderungen an eine/einen CISO können Personen mit grundlegendem, technischen Verständnis und entsprechender Kommunikationskompetenz in Kursen vermittelt werden. Ernannte CISOs bedürfen jedenfalls einer kontinuierlichen Fortbildung.

Darüber hinaus ist der/die CISO mit einem Mandat und damit verbundener Entscheidungsbefugnis auszustatten, während ein CISO innerhalb der Organisation nur gegenüber der oberen Managementebene weisungsgebunden ist. Weiters muss ein CISO uneingeschränkten Zugang zu den wesentlichen Entscheiderinnen/ Entscheidern der eigenen Organisation haben.

Der/Die CISO kann einzelne Aufgaben an das Informationssicherheitsmanagement-Team delegieren. Die Gesamtverantwortung für die Informationssicherheit verbleibt aber bei dieser Person.

6.1.3.2 Das Informationssicherheitsmanagement-Team

Das Informationssicherheitsmanagement-Team unterstützt den CISO und ist verantwortlich für die Regelung der organisationsweiten Informationssicherheitsbelange sowie für die Erarbeitung von Plänen, Vorgaben, Konzepten und Richtlinien zur Informationssicherheit.

Zu den Aufgaben des Teams zählen typischerweise Unterstützungsarbeiten zu allen Aufgaben des CISO, mit einem Fokus auf:

- die Durchführung des Informationssicherheitsrisikomanagements
- die Pflege und Weiterentwicklung des Richtlinienmanagements (z.B. für Informationssicherheitsrichtlinien)
- die Durchführung des Kennzahlenmanagements bzw. Pflege sowie Weiterentwicklung des Kennzahlensystems
- die Festlegung der Informationssicherheitsziele der Organisation
- die Entwicklung einer organisationsweiten Informationssicherheitspolitik
- die Erstellung des Informationssicherheitskonzeptes
- die Überprüfung des Konzeptes auf Erreichung der Informationssicherheitsziele
- die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen
- die Förderung des Sicherheitsbewusstseins in der gesamten Organisation sowie
- die Festlegung der personellen und finanziellen Ressourcen für Informationssicherheit.

Zusammensetzung des Teams:
Die genaue Festlegung der Zusammensetzung sowie der Aufgaben und Verantwortlichkeiten des Informationssicherheitsmanagement-Teams haben im Rahmen der Informationssicherheitspolitik zu erfolgen.

Generell ist zu empfehlen, dass die CISOs sowie ein/e VertreterIn der IT-AnwenderInnen dem Informationssicherheitsmanagement-Team angehören. Idealerweise ist der/die StellvertreterIn der/des CISO ebenfalls Mitglied des Informationssicherheitsmanagement-Teams.

6.1.3.3 Der/Die Informationssicherheitskoordinator/in im Bereich

Die Komplexität moderner IT-Systeme erfordert zur Gewährleistung eines angemessenen Sicherheitsniveaus tiefgehende Systemkenntnisse. Wenn mehrere unterschiedliche Systemplattformen zum Einsatz kommen, können diese von einer einzelnen Person oft nicht mehr abgedeckt werden. Daher wird es in vielen Fällen empfehlenswert sein, Informationssicherheitskoordinatoren/koordinatorinnen zu definieren.

Im Bereich der Informationssicherheit (IS) haben IS-Koordinatoren bzw. IS-Koordinatorinnen (auch abgekürzt als: ISKoord) die fachliche Verantwortung für alle IT-Sicherheitsbelange in einem bestimmten Bereich (z.B. Fachbereich). In organisatorischer Form ist ein Bereich als Zuordnung nach Abteilungen oder Betriebsstandorten denkbar. Ein Bereich kann beispielsweise in technischer Form auch ein IT-System oder eine Betriebssystemplattform umfassen.

Zu den Aufgaben des/der ISKoord zählen

- die Mitwirkung bei den ihren Bereich betreffenden Teilen des Informationssicherheitskonzeptes
- die Erarbeitung eines detaillierten Plans zur Realisierung der ausgewählten Sicherheitsmaßnahmen
- die Umsetzung dieses Plans
- die regelmäßige Prüfung der Wirksamkeit und Einhaltung der eingesetzten Sicherheitsmaßnahmen im laufenden Betrieb
- Information der/des CISO über bereichsspezifischen Schulungsbedarf sowie
- Meldungen an die/den CISO bei sicherheitsrelevanten Ereignissen.

6.1.3.4 Applikations-/Projektverantwortliche

Für jede IT-Anwendung und jedes IT-Projekt ist die fachliche Gesamtverantwortung und damit auch die Verantwortung für deren Sicherheit klar festzulegen.

Zu den Aufgaben der Applikations- oder Projektverantwortlichen zählen insbesondere

- die Sicherstellung der Sicherheits- und Qualitätsanforderungen der Applikation bzw. des Projekts
- die Klassifizierung der verarbeiteten Daten,
- die Vergabe von Zugriffsrechten sowie
- organisatorische und administrative Maßnahmen zur Gewährleistung der IT-Sicherheit in der Projektentwicklung und im laufenden Betrieb.

Neben den oben beschriebenen Rollen gibt es im Bereich der Bundesverwaltung eine spezielle, per Gesetz festgelegte Rolle: die/den Informationssicherheitsbeauftragte/n.

6.1.3.5 Die/Der Informationssicherheitsbeauftragte

Auf Ressortebene sind gemäß Informationssicherheitsgesetz Informationssicherheitsbeauftragte zu bestellen.

Aufgaben der/des Informationssicherheitsbeauftragten sind:

- die Unterstützung der/des CISO,
- die Überwachung der Einhaltung der Bestimmungen des Informationssicherheitsgesetzes, der Informationssicherheitsverordnung und der sonstigen dazugehörigen Informationssicherheitsvorschriften,
- die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von (lt. Informationssicherheitsgesetz) klassifizierten Informationen,
- die Berichterstattung darüber an die Informationssicherheitskommission,

- Behebung von erkannten Mängeln,
- Sicherheitsüberprüfung von betroffenen Personen gemäß §3 Abs. 1 Z1 und 2 Informationssicherheitsgesetz,
- Information der Bundesministerin bzw. des Bundesministers des jeweiligen Ministeriums in Angelegenheiten der Informationssicherheit sowie
- Erstattung von Verbesserungsvorschlägen, falls erforderlich.

Die/Der Informationssicherheitsbeauftragte ist Mitglied der Informationssicherheitskommission.

6.1.3.6 Weitere Pflichten und Verantwortungen im Bereich Informationssicherheit

Sicherheit ist nicht ausschließlich Angelegenheit der damit per Definition betrauten Personen. Alle MitarbeiterInnen, auch wenn sie nicht direkt in den Bereich Informationssicherheit involviert sind, müssen ihre spezifischen Pflichten und Verantwortlichkeiten im Rahmen der Informationssicherheit kennen und erfüllen. Ebenso sind die Rechte und Pflichten von externen Personen, Lieferanten und VertragspartnerInnen festzulegen.

Im Rahmen der organisationsweiten Informationssicherheitspolitik sind daher auch die Aufgaben und Verantwortlichkeiten folgender Personenkreise zu definieren:

- Management/Behördenleitung („Sicherheit als Managementaufgabe“)
- Datenverarbeitungs(DV)-Entwicklung und technischer Support
- DienstnehmerInnen
- Leasingpersonal, externe MitarbeiterInnen
- Lieferanten und VertragspartnerInnen

6.1.3.7 Informationssicherheit und Datenschutz

Das Datenschutzgesetz (DSG) und die DSGVO geben vor, wann ein Datenschutzbeauftragter verpflichtend zu benennen ist. Unabhängig von diesen Verpflichtungen kann ein solcher auch freiwillig in der Organisation etabliert werden. Dadurch können datenschutzbezogene Aufgaben konzentriert und effizienter überwacht bzw. nachvollzogen werden. Es ist aber zu betonen, dass die Gesamtverantwortung für die Datenschutzbelange bei der Geschäftsführung verbleibt und nicht delegiert werden kann.

6.1.4 Definierte Verantwortlichkeiten für Informationssicherheit

Um zu einer umfassenden Gesamtsicherheit zu gelangen, ist die Beteiligung aller MitarbeiterInnen einer Organisation an der Umsetzung der notwendigen Sicherheitsmaßnahmen erforderlich. Es muss festgelegt werden, wer für Informationen, Anwendungen und IT-Komponenten sowie für deren Sicherheit verantwortlich ist. Hierfür sollte immer eine konkrete Person (inklusive VertreterIn) und keine abstrakte Gruppe benannt werden, damit die Zuständigkeit jederzeit deutlich erkennbar ist. Bei komplexeren Informationen, Anwendungen und IT-Komponenten sollten alle Verantwortlichen und deren VertreterInnen namentlich genannt sein.

Umgekehrt sollten natürlich alle MitarbeiterInnen wissen, für welche Informationen, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind.

Alle MitarbeiterInnen sind dabei für das verantwortlich, was in ihrem Einflussbereich liegt, es sei denn, es ist explizit anders geregelt. Beispielsweise ist die Leitungsebene der Organisation verantwortlich für alle grundsätzlichen Entscheidungen bei der Einführung einer neuen Anwendung, der/die LeiterIn der IT zusammen mit dem Informationssicherheitsmanagement für die Ausarbeitung von Sicherheitsvorgaben für die IT-Komponenten, die AdministratorInnen für deren korrekte Umsetzung und die BenutzerInnen für den sorgfältigen Umgang mit den zugehörigen Informationen, Anwendungen und Systemen.

Die Fachverantwortlichen als die „Eigentümer“ von Informationen und Anwendungen müssen sicherstellen, dass

- der Schutzbedarf der Informationen, Anwendungen und IT-Komponenten korrekt festgestellt wurde,
- die erforderlichen Sicherheitsmaßnahmen umgesetzt werden,
- dies regelmäßig (z. B. täglich, wöchentlich, monatlich) überprüft wird,
- die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen klar definiert und zugewiesen werden,
- der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt ist,
- Abweichungen, welche die Informationssicherheit gefährden, schriftlich dokumentiert werden.

Die Fachverantwortlichen müssen zusammen mit dem Informationssicherheitsmanagement entscheiden, wie mit eventuellen Restrisiken umgegangen wird.

Siehe dazu auch 6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit.

[Quelle: BSI IT-Grundschutz]

6.1.5 Benutzungsgenehmigung für Informationsverarbeitung

Beschaffung, Installation und Betrieb von informationsverarbeitenden Komponenten aller Art muss koordiniert und genehmigt sein. Dies betrifft die geregelte Abnahme, Freigabe, Installation und Benutzung von Komponenten wie auch etwa externen Laufwerken, USB-Sticks, Mobiltelefonen und Software.

Die Regelung muss den gesamten Lebenszyklus der jeweiligen Komponente umfassen, also je nach Eigenschaften und Sicherheitsrelevanz:

- Erstellung eines Anforderungskataloges
- Auswahl eines geeigneten Produktes
- Funktions- und Kompatibilitätstest
- Freigabe
- Installation
- Lizenzverwaltung
- Deinstallation
- Entsorgung/Vernichtung

Notwendigkeit zur Koordination und Genehmigung betrifft auch Wartungsaktivitäten an bestehenden sicherheitsrelevanten Einrichtungen, wenn sich Änderungen auf die Sicherheit des Gesamtsystems auswirken könnten.

Ebenfalls muss die allfällige Verwendung von persönlichen oder privaten Informationsverarbeitungs-Einrichtungen geregelt werden, wenn sie auch Geschäftsinformationen verarbeiten sollen (weit verbreitet sind Kalender und Telefonlisten auf Mobiltelefonen): Diese können erhebliche Schwachstellen bedeuten, weiters ist bei diesen dann oft unklar, wer der Eigentümer der Information ist. Da sie praktisch sind und in vielen Fällen von der Managementebene benutzt werden, sind generelle Verbote ihres Einsatzes zunehmend schwieriger umzusetzen. Stattdessen müssen exakte Policies ihrer Verwendung und notwendiger Maßnahmen (etwa Verschlüsselung) definiert und umgesetzt werden. Siehe dazu auch 6.3.1 Mobile IT-Geräte.

Jedenfalls muss vor der Genehmigung von Komponenten

- ihre Funktionstüchtigkeit,
- ihre Sicherheitseigenschaften,
- mögliche durch ihren Einsatz entstehende Sicherheitsrisiken,
- allfällige Einsatzbedingungen und zu erarbeitende Installationsanweisungen

bekannt sein.

Während des Genehmigungsverfahrens sollten außerdem Installations- bzw. Konfigurationsanleitungen erarbeitet werden, in denen auch alle sicherheitsrelevanten Einstellungen dokumentiert sind. Auch nach der Erstinstallation von Komponenten müssen diese weitergepflegt werden. Vor der Inbetriebnahme neuer Komponenten sind (sofern erforderlich) die AdministratorInnen bzw. die BenutzerInnen in deren Anwendung zu schulen.

Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.

Siehe dazu auch

- 14.1.6 (ff) Testen von Software bis
- 14.1.11 Deinstallation von Software sowie
- 14.3.1 Nutzungsverbot nicht freigegebener Software und
- 14.3.2 Nutzungsverbot privater Hard- und Softwarekomponenten.

[Quelle: BSI IT-Grundschutz]

6.1.6 Kontaktpflege mit Behörden und Gremien

> *Rasche Kontaktaufnahme mit zuständigen Behörden oder Versorgungseinrichtungen (Feuerwehr, Polizei, Aufsicht, aber auch Wasser-, Elektrizitäts- und Gasversorgungsunternehmen sowie Internet- oder Telekombetreiber) ist insbesondere bei Notfällen, Sicherheitsvorfällen oder Verdacht auf kriminelle Handlungen von entscheidender Bedeutung.*

Daher sollen zum einen rechtzeitig Pläne, Verfahren und Kontaktlisten erstellt werden, damit rasch und zuverlässig die richtigen AnsprechpartnerInnen kontaktiert und ggf. eingewiesen werden können. Dies ist eine Aufgabe des Incident Handlings (siehe dazu 16.1.4 Prioritäten bei der Behandlung von Sicherheitsvorfällen).

Zum anderen sollten regelmäßige, ggf. auch informelle Beziehungen zu solchen Institutionen gepflegt werden. Damit können beispielsweise Vorsorgemaßnahmen vorab abgestimmt oder relevante Neuerungen bekanntgegeben werden, resp. kann die Organisation auf neue Gegebenheiten (etwa Vorschriften) angepasst werden.

Sinnvoll ist auch die Teilnahme oder Mitgliedschaft in Interessens-, Arbeits- bzw. Expertengremien. Damit wird nicht nur der eigene Wissensstand betreffend Technologien, Produkten, Gefährdungen, Best Practices und anderer Bereiche erhöht, sondern ein gemeinsamer Wissensstand mehrerer Partner aufgebaut, der in der Regel viel umfassender ist. In solchen Gremien sind meist rasch und unkompliziert Sicherheitswarnungen und Informationen über bereits erprobte Behebungsmaßnahmen, resp. generell Zugang zu Expertenwissen, zu bekommen.

Weiters können über solche geeignete Gremien oder Foren neue oder zusätzliche AnsprechpartnerInnen für Problemlösungen bzw. Behandlung von Sicherheitsvorfällen gefunden, bzw. die Kontakte mit ihnen gepflegt werden. Dazu ist es sinnvoll, einen Überblick über passende Gremien und Interessensgruppen zu haben und zu entscheiden, in welchen aktiv mitgearbeitet oder lediglich Ergebnisse beobachtet werden.

Allerdings ist zu beachten, dass sensible Informationen auch gegenüber Gremien oder Kontaktpersonen geschützt bleiben müssen. Entweder dürfen sie also nicht verwendet werden, oder es müssen geeignete Vertraulichkeitsvereinbarungen abgeschlossen werden.

6.2 Zusammenarbeit mit Externen

6.2.1 Outsourcing

> *Outsourcing bedeutet, dass Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert und von diesen durchgeführt werden. Ob dies in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters geschieht, ist nicht erheblich.*

Beispiele:

- Nutzung und Betrieb von Hardware und Software
- Betrieb eines Rechenzentrums, einer Applikation, einer Website
- Wachdienst

Ausgelagerte Dienstleistungen mit Bezug zur IT-Sicherheit heißen „Security Outsourcing“ oder „Managed Security Services“:

- ausgelagerter Firewall-Betrieb
- Netzwerküberwachung
- Virenschutz
- Betrieb eines Virtual Private Networks (VPN)

Dienstleister, die auf ihren eigenen Systemen Anwendungen für ihre Kunden betreiben, heißen „Application Service Provider“ (ASP):

- E-Mail
- SAP-Anwendungen
- Archivierung
- Web-Shops

Sind die Anwendungen Eigentum des Kunden, spricht man von „Application Hosting“.

Meist sind Auftraggeber und Dienstleister über das Internet oder ein VPN miteinander verbunden.

Die Erwartung an Outsourcing von Geschäftsprozessen oder Produktionen sind unter Anderem:

- Konzentration auf Kernkompetenz (Core Business)
- Kostenersparnis (etwa IT-Systeme samt Personal)
- Entlastung eigener Ressourcen
- Flexibilität der Prozesse

Obwohl auch einige Outsourcing-Projekte gescheitert sind, besteht nach wie vor ein Trend zu verstärkter Auslagerung.

Eine Herausforderung für die Informationssicherheit liegt darin, dass die Informationssysteme und Netzwerke der eigenen Organisation und ihrer Dienstleister miteinander verbunden werden. Der Ablauf eigener Geschäftsprozesse wird nun vom Dienstleister gesteuert und es entsteht eine Abhängigkeit von dessen Qualität. Damit ergeben sich eine Reihe von potenziell höchst gefährlichen bzw. existenzgefährdenden Risiken für die auftraggebende Organisation.

Wesentlich sind daher beim Outsourcing die Kenntnis und Behandlung der Gefährdungen bzw. Sicherheitmaßnahmen sowie die Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Dienstleister.

[Quelle: BSI B 1.11]

6.2.2 Gefährdungen beim Outsourcing

Die Gefährdungslage eines Outsourcing-Vorhabens ist ausgesprochen vielschichtig. Die Entscheidung über das Auslagern einer speziellen Aktivität beeinflusst nachhaltig die strategische Ausrichtung der Organisation, die Definition ihrer Kernkompetenzen, die Ausgestaltung der Wertschöpfungskette und betrifft viele weitere wesentliche Belange eines Organisationsmanagements. Es sollten daher alle Anstrengungen unternommen werden, um Fehlentwicklungen der eigenen Organisation frühzeitig zu erkennen und zu verhindern.

Die Gefährdungen können parallel auf physikalischer, technischer und auch menschlicher Ebene existieren und sind nachfolgend in den einzelnen Gefährdungskatalogen aufgeführt. Um die jeweils existierenden Risiken quantitativ bewerten zu können, müssen zuvor die organisationseigenen Werte und Informationen entsprechend ihrer strategischen Bedeutung für die Organisation beurteilt und klassifiziert werden.

- Höhere Gewalt

- Ausfall eines Wide Area Netzwerkes
- Organisatorische Mängel
- Fehlende oder unzureichende Regelungen
- Unerlaubte Ausübung von Rechten
- Fehlendes oder unzureichendes Test- und Freigabeverfahren
- Ungesicherter Akten- und Datenträgertransport
- Unzureichendes Sicherheitsmanagement
- Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
- Fehlerhafte Outsourcing-Strategie
- Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
- Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens
- Abhängigkeit von einem Outsourcing-Dienstleister
- Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
- Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase
- Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
- Unzureichendes Notfallvorsorgekonzept beim Outsourcing
- Menschliche Fehlhandlungen
- Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
- Technisches Versagen
- Schlechte oder fehlende Authentifikation
- Ausfall eines Kryptomoduls
- Ausfall der Systeme eines Outsourcing-Dienstleisters
- Vorsätzliche Handlungen
- Missbrauch von Fernwartungszugängen
- Missbrauch von Administratorrechten
- Social Engineering
- Vertraulichkeitsverlust schützenswerter Informationen
- Integritätsverlust schützenswerter Informationen
- Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

[Quelle: BSI B 1.11]

6.2.3 Outsourcing-Planungs- und -Betriebsphasen

Ein ausgelagerter Geschäftsprozess oder ein damit zusammenhängender IT-Verbund kann sowohl aus Komponenten bestehen, die sich ausschließlich im Einflussbereich des Outsourcing-Dienstleisters befinden, als auch aus Komponenten beim Auftraggeber. In der Regel gibt es in diesem Fall Schnittstellen zur Verbindung der Systeme des Auftraggebers sowie des Outsourcing-Dienstleisters. Für jedes Teilsystem und für die Schnittstellenfunktionen muss das definierte Sicherheitsniveau gewährleistet sein.

Phase 1: Strategische Planung des Outsourcing-Vorhabens

Schon bei der Entscheidung, ob und in welcher Form ein Outsourcing-Vorhaben umgesetzt wird, müssen die sicherheitsrelevanten Gesichtspunkte herausgearbeitet werden.

Outsourcing zieht wirtschaftliche, technische, organisatorische und sicherheitsrelevante Aspekte nach sich und bedingt vorab:

- Unternehmensstrategie
- Machbarkeitsstudie mit den Rahmenbedingungen
- Kosten-Nutzen-Schätzung
- Welche Geschäftsprozesse oder Anwendungen sollen ausgelagert werden (Kerngeschäft, Routineabläufe)?
- Wie können weiters Anforderungen an die IT gestellt werden?
- Was geschieht mit bisher selbst entwickelten IT-Anwendungen?

Wesentlich ist zunächst die Klärung, ob Auslagerungen von Aufgaben rechtlich möglich bzw. aufgrund von Auflagen schwierig sein werden (etwa gesetzlich festgeschriebene Kompetenzen, Gewerbeberechtigungen, Konzessionen, Einschaltung von Aufsichtsbehörden). Es muss klar sein, dass die Verantwortung für Produkte oder Dienstleistungen bei der eigenen Organisation verbleibt, mitunter aber durch Auslagern mit höherem Risiko - sowie weiteren Risiken - verbunden sein kann:

- Outsourcing kann in der Regel nicht einfach rückgängig gemacht werden, es entsteht eine langfristige Bindung an den Dienstleister (sog. „Vendor Lock-In“).
- Der Dienstleister hat Zugriff auf Informationen bzw. auf Daten und IT-Ressourcen der eigenen Organisation. Sie verliert die alleinige und vollständige Kontrolle darüber und muss die Zugangsberechtigungen für den Dienstleister der zu Ihren Systemen Zugang hat verwalten.
- Datenübertragung vom und zum Dienstleister erzeugt neue Gefährdungen und erfordert die Klärung welche Daten zum Dienstleister übertragen werden dürfen und welche nicht, sowie deren Klassifizierung.
- Meist ist es notwendig, dass MitarbeiterInnen des Dienstleisters oder von Subunternehmen zumindest zeitweise in den Räumlichkeiten der eigenen Organisation arbeiten müssen.

- Im Rahmen des Outsourcing werden neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt und bewirken Änderungen des Sicherheitskonzepts und der Implementierungen.
- Ein häufiger Grund, IT-Dienstleistungen auszulagern, ist einerseits die Spezialisierung der Dienstleister und andererseits die Erwartung von Kostensenkungen - bei gleicher oder gar besserer Qualität. Es muss vorab abgeschätzt werden, wieso das dem Dienstleister gelingen wird, wenn er dabei auch noch einen Gewinn lukriert. Selbstverständlich gibt es viele Fälle, wo dies tatsächlich möglich ist, etwa durch gute Auslastung großer Installationen.
- Ein gewisser Know-how Transfer zum Dienstleister lässt sich (auch mit „wasserdichten“ Vertraulichkeitsvereinbarungen) nicht verhindern, da bei dessen MitarbeiterInnen entsprechendes Wissen aufgebaut wird.

Die IT-Sicherheit sollte keinesfalls bei den strategischen Überlegungen vernachlässigt werden. Daher sollte eine Sicherheitsanalyse durchgeführt werden, um festzustellen, wie bestehende IT-Systeme oder IT-Verbünde abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können:

- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Feststellung des Handlungsbedarfs sowie der erwarteten Kosten für umzusetzende Maßnahmen

Bei hohem Schutzbedarf wichtiger Systeme oder Anwendungen muss eine ergänzende Sicherheitsanalyse (z. B. Risikoanalyse) durchgeführt werden. Meist wird ein zusätzliches Restrisiko bei der eigenen Organisation verbleiben. Dieses Restrisiko bzw. diese Restrisiken müssen durch das Management getragen werden. Schließlich erfolgt die Dokumentation der Outsourcing-Strategie mit Zielen, Chancen und Risiken sowie den Erfahrungen.

[Quelle: BSI M 2.250]

Phase 2: Definition der wesentlichen Sicherheitsanforderungen

Wenn die Entscheidung zum Outsourcing gefallen ist, müssen die wesentlichen übergeordneten Sicherheitsanforderungen für das Outsourcing-Vorhaben festgelegt werden. Diese Sicherheitsanforderungen sind die Basis für das Ausschreibungsverfahren.

Mit dem ausgelagerten Betrieb ergeben sich neue Sicherheitsanforderungen sowohl an den auszuwählenden Dienstleister wie auch an die eigene Organisation. Diese werden zunächst beginnend mt den gewünschten Sicherheitsniveaus in den betroffenen Bereichen immer weiter verfeinert, um dann konkret genug zu sein, einen geeigneten Dienstleister auszuwählen. Auch nach erfolgter Auswahl wird eine weitere Verfeinerung der Sicherheitsanforderungen bis hin zu den Umsetzungsschritten notwendig sein.

Folgende Aspekte sind in der Regel zu berücksichtigen:

- Welches Mindestniveau (IT-Grundschutz oder ISO/IEC 27001) ist von beiden Parteien zu erfüllen?
- Sowohl Dienstleister wie eigene Organisation müssen über ein Sicherheitskonzept verfügen und dieses umgesetzt haben.
- Es entstehen Schnittstellen zwischen den nun im Verbund wirkenden Aufgaben, Geschäftsprozessen, Anwendungen und Systemen. Diese müssen identifiziert und beschrieben werden.
- An diese Schnittstellen müssen technische und organisatorische Sicherheitsanforderungen gestellt werden.
- Strukturanalyse und Schutzbedarfsfeststellung (IT-Systeme, Anwendungen, Kommunikationsverbindungen, Räume) hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit müssen erfolgen.
- Notwendige Einräumung von Zutritts- und Zugriffsrechten (z.B. zu Büroräumen, Rechenzentrum) für den Dienstleister je nach Bedarf und regelmäßige Auditierung dieser Berechtigungen.
- Aufzeigen der Auswirkungen relevanter Gesetze und Vorschriften. Dies kann erheblichen Aufwand verursachen, etwa bei länderübergreifendem Outsourcing oder wenn einer oder beide Partner weltweit tätig sind sowie wenn die Infrastruktur des Partners auf geographisch weit voneinander entfernte Standorte verteilt ist.
- Beschreibung der Anforderungen an Infrastruktur, Organisation, Personal und Technik durch das zu erreichende Sicherheitsniveau (etwa auch Alarmierungen, Benennung von Sicherheitsbeauftragten beim Dienstleister).
- Spezielle Anforderungen an Hard-/Software (etwa zertifizierte Produkte beim Dienstleister).
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen (Service Levels, Lastverteilung etwa bei Web-Servern).
- Vorgaben an die Mandantenfähigkeit und ggf. Trennung von Hard- und Software (etwa keine Systeme anderer Mandanten im gleichen Raum des Dienstleisters, exklusiv genutzte Hardware in Käfigen).
- Vorgaben zur Absicherung der Kommunikation zwischen Dienstleister und eigener Organisation (Verschlüsselungs- und Signaturverfahren).
- Anforderungen zur Qualitätssicherung (etwa Messungen von Reaktionszeiten, Verfügbarkeit).
- Spezifizieren von gewünschten Verfahren für die Kontrolle und Überwachung (etwa unangekündigte Kontrollen vor Ort, Audits - ggf. durch unabhängige Dritte).
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien.

[Quelle: BSI M 2.251]

Phase 3: Auswahl des Outsourcing-Dienstleisters

Ihr kommt eine besondere Bedeutung zu, etwa da langfristige Abhängigkeiten entstehen.

Kritische Erfolgsfaktoren dafür, dass sich geeignete Dienstleister bewerben, sind:

- möglichst detailliertes Anforderungsprofil
- darauf basierendes Pflichtenheft

Eine bedarfsgerechte Ausschreibung sollte enthalten:

- Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung)
- Beschreibung des geforderten Qualitätsniveaus (dieses kann ggf. anders sein als das der eigenen Organisation)
- Anforderungen an die Informationssicherheit
- Kriterien zur Messung von Servicequalität und Sicherheit
- Anforderungen an die Qualifikation der MitarbeiterInnen. Sicherstellung, dass diese dann tatsächlich tätig sind und dass es geeignete VertreterInnen gibt
- Bei ausländischen Dienstleistern: Festlegung der Sprache für die gemeinsame Kommunikation und Sicherstellung, dass diese von allen befassten MitarbeiterInnen (auch den eigenen) auch in Detailaspekten beherrscht wird
- Notwendigkeit bzw. Vorliegen von Sicherheitsüberprüfungen der MitarbeiterInnen des Dienstleisters

Zu beachten ist, dass aus detallierten Sicherheitsanforderungen Schlüsse auf die eigenen Sicherheitsmechanismen und ihre Wirksamkeit gezogen werden können. Daher kann es notwendig sein, diese nur gegen Vertraulichkeitsvereinbarung an den sich bewerbenden Dienstleister zu übermitteln.

[Quelle: BSI M 2.252]

Phase 4: Vertragsgestaltung

Auf Basis des Pflichtenheftes muss nun ein Vertrag mit dem Partner ausgehandelt werden, der die gewünschten Leistungen inklusive Qualitätsstandards und Fristen im Einklang mit der vorhandenen Gesetzgebung festschreibt. Diese Verträge werden häufig als Service Level Agreements (SLAs) bezeichnet. In diesem Vertrag müssen auch die genauen Modalitäten der Zusammenarbeit geklärt sein: Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der IT-Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen, Verwertungsrechte, Weitergabe von Information an Dritte etc.

Dabei ist es empfehlenswert, die vereinbarten Leistungen und Ziele so genau und eindeutig wie möglich vertraglich festzuhalten. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretationen der beschriebenen Leistungen notwendig werden, sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden. Auch die Erstellung des IT-Sicherheitskonzeptes selbst sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen. Ggf. kann und sollte sich der Auftraggeber ein Mitspracherecht einräumen lassen, welches Personal der Dienstleister einsetzen wird (Qualifikation, Sicherheitsüberprüfung, Sprachkenntnisse).

[Quelle: BSI M 2.253]

Phase 5: Erstellung eines IT-Sicherheitskonzepts für den ausgelagerten IT-Verbund

Auftraggeber und Outsourcing-Dienstleister müssen ein detailliertes Sicherheitskonzept, das auch ein Notfallvorsorgekonzept enthält, erstellen.

Bei Outsourcing-Projekten ergeben sich viele technische und organisatorische Details erst im Laufe der Planung und der Migration der Systeme. Daher wird das Sicherheitskonzept für das Outsourcing-Vorhaben in den wenigsten Fällen gleich vollständig und endgültig sein, sondern muss während der Migration stetig weiterentwickelt und konkretisiert werden.

Sicherheitskonzepte für Outsourcing-Vorhaben unterscheiden sich in einigen Punkten von solchen für eigene Systeme, da in der Regel 3 technische Parteien beteiligt sind:

- 1. Outsourcing-Auftraggeber
- 2. Outsourcing-Dienstleister
- 3. Netzprovider (Anbindung zwischen den Outsourcing-Parteien - zuständig für die Netzanbindung ist in der Regel der Outsourcing-Dienstleister).

Jeder Beteiligte muss ein Sicherheitskonzept in seinem jeweiligen Einflussbereich erstellen und umsetzen (im Fall des Netzproviders sind die Schnittstellen relevant).

Darüber hinaus muss dann ein IT-Sicherheitskonzept für das Gesamtsystem erstellt und mit den Teilkonzepten abgestimmt werden, aus welchem die Sicherheit im Zusammenspiel der Einzelsysteme hervorgeht. Am Sicherheitskonzept des Outsourcing-Dienstleisters ist der Auftraggeber nicht direkt beteiligt, sollte aber in einem Audit - ggf. durch externe Dritte - prüfen, ob es vorhanden und ausreichend ist. Besondere Aufmerksamkeit ist dabei auch auf die Migrationsphase der Aufgaben und Systeme zum Dienstleister zu richten, da während dieser mit Sicherheitsvorfällen gerechten werden muss. Einige Themen und Aspekte für das Outsourcing-Sicherheitskonzept:

Organisation

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen/Vernichten
- Festlegung von Aktionen, für die das „Vier-Augen-Prinzip“ anzuwenden ist

Hard-/Software

- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
- Einsatz von Datei-Integrität-Prüfungssystemen, um Veränderungen z. B. nach erfolgreichen Angriffen, zu erkennen
- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
- Einsatz kaskadierter Firewallsysteme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters
- Sorgfältige Vergabe von Benutzerkennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters

Kommunikation

- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Auftraggeber, um sensitive Daten zu schützen
- Authentisierungsmechanismen
- Detailregelungen für weitere Netzanbindungen
- Detailregelungen für den Datenaustausch

Kontrollen und Qualitätssicherung

- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Sicherheit, Dienstqualität, Abläufen und organisatorische Regelungen

Notfallvorsorge

Beim Outsourcing-Betrieb ist auch die Notfallvorsorge auf unterschiedliche Parteien aufgeteilt und die IT-Komponenten sind verteilt.

Notfallvorsorgekonzepte müssen für die Systeme beim Auftraggeber, beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Auftraggeber und Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren und detailliert beschreiben:

- Regelung und Dokumentation von Zuständigkeiten, Ansprechpartnern und Abläufen
- Erstellen von Detailregelungen für die Datensicherung (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz)
- Erstellen von Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen
- Konzeption von regelmäßig durchzuführenden Notfallübungen

Eine besodere Problematik kann sich dadurch ergeben, dass das Personal des Dienstleisters meist keine inhaltlichen Kenntnisse über die Anwendungen besitzt, die auf seinen Systemen betrieben werden, aber Fehler beheben soll oder muss. Daher sind genaue Anweisungen seitens des Auftraggebers erforderlich:

- wie bei Fehlern vorzugehen ist
- welche Aktionen erlaubt resp. verboten sind
- auf welche anwendungsspezifischen Informationen zurückgegriffen werden kann
- ob und welche Schutzmaßnahmen für solche Informationen einzuhalten sind
- welche Anprechpartner beim Auftraggeber für anwendungsspezifische Probleme zur Verfügung stehen

Ein weiteres Problem kann sich durch Fortpflanzung eines Anwendungsfehlers auf andere Anwendungen ergeben. Die kann der Dienstleister meist nicht selbst abschätzen und muss daher rechtzeitig mit dem Auftraggeber Kontakt aufnehmen.

Phase 5 wird in der Regel erst nach Beendigung der Migrationsphase abgeschlossen werden können, weil sich während der Migration der IT-Systeme und Anwendungen immer wieder neue Erkenntnisse ergeben, die in das IT-Sicherheitskonzept eingearbeitet werden müssen.

[Quelle: BSI M 2.254, M 6.83]

Phase 6: Migration - Übergang der Anwendungen und Systeme zum Dienstleister

> *Besonders sicherheitskritisch ist die Migrations- oder Übergangsphase, die deshalb einer sorgfältigen Planung bedarf.*

In einem zu erarbeitenden vorläufigen Sicherheitskonzept müssen die Test- und Einführungsphase als Teil des gesamten Vorhabens betrachtet werden:

- in dieser Phase sind zahlreiche Betriebsfremde involviert,
- es müssen Abläufe etabliert, Aufgaben übertragen und
- Systeme neu eingerichtet bzw. angepasst werden

Bei Tests in Zeiten großer Arbeitsbelastung werden gerne „quick and dirty“ Lösungen gewählt, die selten sehr sicher sind (z. B. werden Kopien von Produktionsdaten ohne weiteren Schutz verwendet).

In der eigenen Organisation sollte ein Sicherheitsmanagement-Team speziell für die Umstellungsphase eingerichtet werden und schon vor der Umstellung für sicheren IT-Betrieb während der Migrationsphase sorgen. Seine Größe hängt vom Vorhaben ab, zumindest sollte es aus einem Sicherheitsexperten bestehen und hat die Aufgaben:

- Zusammenstellung eines gemischten Teams aus MitarbeiterInnen des Auftraggebers und des Outsourcing-Dienstleisters, ggf. zusätzlich mit externen ExpertInnen.
- Erarbeiten eines Sicherheitskonzeptes für die Umstellungsphase.
- Festlegen der Verantwortlichkeiten für die Umstellungsphase - mit klaren Führungsstrukturen und eindeutigen AnsprechpartnerInnen auf beiden Seiten - auch auf oberer Managementebene.
- Planung und Durchführung der erforderlichen Tests und Abnahmeprozeduren.
- Planung der Produktionsumstellung.
- Auswahl geeigneter interner MitarbeiterInnen für die Test-, die Einführungsphase und den späteren Betrieb (ggf. vertragliches Mitspracherecht des Auftraggebers).
- Schulung der MitarbeiterInnen des Auftraggebers über Abläufe und Verhalten während und nach der Umstellung. Da sie dabei mit neuen und unbekannten AnsprechpartnerInnen konfrontiert sind, entsteht eine Gefahr des „Social Engineerings“ (z. B. Anruf von vermeintlichen MitarbeiterInnen des Sicherheitsteams des Dienstleisters).
- Einweisung des Dienstleisters auf die relevanten Abläufe, Applikationen und IT-Systeme des Auftraggebers.
- Ressourcenplanung und Tests, ohne die laufenden Systeme zu vernachlässigen. Sicherstellung, dass die vorgesehenen MitarbeiterInnen zur Verfügung stehen (ggf. Urlaubssperren). Störungen durch Tests und dabei auftretende Fehler müssen einkalkuliert werden.
- Prüfung der Dokumentation, die der Dienstleister übernehmen soll, auf Vollständigkeit und Aktualität; ggf. Anpassung auf neue Gegebenheiten durch das Outsourcing.
- Laufende Überprüfung, ob durch Erkenntnisse aus der Umstellung Verträge (Service Level Agreements) oder vorgesehene Sicherheitsmaßnahmen angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen eingestellt hat, sind ggf. MitarbeiterInnen zu zusätzlichen Bereitschaftsdiensten heranzuziehen.

Nach der Umstellung/Migration muss das Sicherheitskonzept auf Basis der Erfahrungen und Änderungen während der Umstellungsphase aktualisiert werden:

- Konkrete Darstellung aller Sicherheitsmaßnahmen
- Ansprechpartner und Zuständigkeiten mit Namen und notwendigen Kontaktdaten, Erreichbarkeitszeiten
- Dokumentation der Systemkonfigurationen inkl. Einstellungen sicherheitsrelevanter Parameter
- Schulungen für das Personal auf den Regelbetrieb

[Quelle: BSI M 2.255]

Phase 7: Planung und Sicherstellen des laufenden Betriebs

Nach Übernahme der Systeme bzw. der Geschäftsprozesse durch den Outsourcing-Dienstleister sind Maßnahmen zur Gewährleistung der IT-Sicherheit im laufenden Betrieb notwendig und müssen bereits im Vorfeld - inklusive Notfall und Eskalationsszenarien - geplant worden sein. Dies sollte in einem Oursourcing-Betriebskonzept erfolgen.

Die einzelnen Aufgaben unterscheiden sich zwar nicht grundsätzlich vom Betrieb innerhalb der eigenen Organisation, durch die Verteilung auf mehrere Partner und zusätzlichem Abstimm- bzw. Kontrollbedarf entstehen allerdings Besonderheiten:

- Regelmäßige Aktualisierungen von Richtlinien und Dokumentationen
- Regelmäßige Überprüfungen der Sicherheitskonzepte aller Beteiligten, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten
- Auswirkungen von Änderungen im Einflussbereich des Dienstleisters und Information darüber an den Auftraggeber

Im Rahmen des ausgelagerten Betriebs sind weiters durchzuführen:

Regelmäßige Kontrollen

- Durchführung der vereinbarten Audits
- Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen
- Wartungszustand von Systemen und Anwendungen
- Rechtezuweisung durch den Dienstleister
- Einsatz von MitarbeiterInnen, die dem Auftraggeber nicht gemeldet wurden, z. B. Vertretungen
- Performance, Verfügbarkeit, Qualitätsniveau
- Datensicherung

Regelmäßige Abstimmungen

- Informationsaustausch zwischen den Partnern über mögliche Auswirkungen auf die Dienstleistung bzw. Sicherheit (z. B. personelle/organisatorische Änderungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen)
- Information über aufgetretene Probleme
- wechselseitiges Feedback und Aufzeigen von Verbesserungspotenzialen
- Motivation der MitarbeiterInnen (etwa positive Beispiele einer gelungenen Kooperation)
- Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf)

Regelmäßige Übungen und Tests

- Reaktion auf Systemausfälle (Teil- oder Totalausfälle)
- Wiederanlauf, Wiedereinspielen von Datensicherungen
- Beherrschung von Sicherheitsvorfällen

[Quelle: BSI M 2.256]

6.3 Mobile Computing und Telearbeit

Mobile IT-Arbeitsplätze mit Notebook, Smartphone, Tablet, …

IT-BenutzerInnen werden immer mobiler und können, dank immer kleinerer und leistungsfähigerer Geräte, nahezu überall arbeiten. Daher werden dienstliche Aufgaben häufig nicht mehr nur in Räumen des Unternehmens bzw. der Behörde wahrgenommen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, beispielsweise im Hotelzimmer, im Zug oder beim Kunden. In solchen Umgebungen kann aber nicht die infrastrukturelle Sicherheit, wie sie in einer gut geschützten, gewerblichen oder behördlichen Büroumgebung anzutreffen ist, vorausgesetzt werden. Daher sind geeignete Sicherheitsmaßnahmen zur Kompensation zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen.

Typische Gefährdungen bei mobilen Arbeitsplätzen sind:

- Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze,
- Beeinträchtigungen durch wechselnde Einsatzumgebungen oder ungenügende Arbeitsbedingungen,
- Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz,
- Verzögerungen durch temporär eingeschränkte Erreichbarkeit,
- Ungesicherter Akten- und Datenträgertransport,
- Ungeeignete Entsorgung der Datenträger und Dokumente,

- Vertraulichkeitsverlust schützenswerter Informationen,
- Diebstahl oder Verlust von Datenträgern oder Dokumenten,
- Umwelteinflüsse (Nässe, Kälte, Hitze),
- Unzureichende Prüfung, Kontrolle bzw. Tests der Sicherheitsmaßnahmen,
- Nichtbeachtung von Sicherheitsmaßnahmen,
- Ungeeigneter Umgang mit Passwörtern,
- Sorglosigkeit im Umgang mit Informationen,
- Manipulation oder Zerstörung von Geräten oder Zubehör,
- Manipulation an Informationen oder Software,
- Vertraulichkeitsverlust schützenswerter Informationen,
- Unbefugter Zutritt zu schutzbedürftigen Räumen,
- Brand oder Wassereintritt (sog. “Höhere Gewalt”).

Auch für mobile Arbeitsplätze sind eine Reihe von Sicherheitsmaßnahmen zum Schutz umzusetzen. Auch diese sollten angelehnt an das angewendete Lebenszyklusmodell durchlaufen werden:

- Planung und Konzeption der Einrichtung eines Arbeitsplatzes in fremder Umgebung.
- Regelungen für alle mobilen Außentätigkeiten, welche Informationen außerhalb der Räume der Organisation transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind. Dabei ist auch zu klären, unter welchen Rahmenbedingungen MitarbeiterInnen mit mobilen IT-Systemen Zugriff auf interne Daten ihrer Organisation bzw. Institution haben dürfen.
- Schaffung und Einhaltung von Regelungen über die Arbeitsumgebung und die sorgfältige sowie sichere Behandlung der mitgenommenen IT-Systeme (z. B. Notebook, Tablet, Smartphone, externe Peripherie wie Backup-Medien, …).
- Sorgfältige Entsorgung von Datenträgern und Papierausdrucken (keinesfalls dürfen sie einfach in den Müll geworfen werden).

Telearbeit

Unter Telearbeit versteht man i. Allg. Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung mittels Fernzugängen an die IT des Arbeitgebers unterstützt wird.

Bei Telearbeit (Bezeichnung nach ISO/IEC 27001) handelt es sich um kurzfristige bis hin zu langfristigen berufliche Tätigkeiten, welchen die MitarbeiterInnen nicht innerhalb der Räumlichkeiten einer Organisation (z.B. Bürostandort, Fabrik, Rechenzentrum) nachgehen und in diesem Zusammenhang unter Verwendung von IKT-Systemen mittels Fernzugängen auf Daten zugreifen oder Ressourcen

innerhalb des Netzwerks dieser Organisation verwenden. Umfasst sind davon sowohl Tätigkeiten mit eingeschränkten Berechtigungen aber auch solche mit privilegierten Rechten wie etwa Wartungsaufgaben oder zu zwecken der Verwaltung von Computersystemen.

Die Geräte zum Verbindungsaufbau bzw. zum Zugriff auf Daten und Ressourcen befinden sich demzufolge außerhalb der Räumlichkeiten einer Organisation (z.B. im „Homeoffice“, auf sog. „Coworking-Spaces“ oder auf Reisen). Oftmals handelt es sich bei Remote-Arbeit um sogenanntes „Homeoffice“, nämlich wenn die Arbeit von einem Wohnsitz oder einem damit vergleichbaren Standort im eigenen Wohnumfeld durchgeführt wird. Hierbei unterscheidet man zwischen ausschließlicher Tele(heim)arbeit (Homeoffice) und alternierender Telearbeit, d. h. die ArbeitnehmerInnen arbeiten teilweise im Büro und teilweise zu Hause.

Telearbeit deckt sowohl die Verwendung und den Zugriff auf Daten in Papierform sowie für elektronische Daten ab. Andererseits ist auch die Nutzung von Applikationen, Computern, IT-Systemen oder Netzwerkressourcen davon betroffen.

Telearbeit erfordert zur Organisation der Informationssicherheit Regelungen zur Abdeckung von Sicherheitsaspekten unter Berücksichtigung der damit verbundenen Risiken und für die Gewährleistung der Datensicherheit umzusetzende Schutzmaßnahmen.

Synonym für Telearbeit finden zumeist folgende alternativen Begriffe Anwendung:

- Arbeiten auf Reisen
- Digitales Arbeiten bzw. Digitaler Workspace
- Fernarbeit
- Flexibler Arbeitsplatz
- Häuslicher Arbeitsplatz (gem. BSI)
- Homeoffice (vgl. § 2h (1) Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG))
- Mobiles Arbeiten bzw. Mobiler Workspace
- Ortsunabhängiges Arbeiten
- Remote-Arbeit
- Virtuelle Arbeitsumgebung

Bei Formen der Telearbeit, die teilweise oder ganz im häuslichen Umfeld durchgeführt werden, besteht in der Regel zwischen dem Arbeitsplatz zu Hause und der Organisation eine Internetverbindung, welche den Austausch von Daten oder ggf. auch den Zugriff auf Daten, die sich im Netzwerk der Organisation befinden, ermöglicht.

Die Maßnahmenempfehlungen dieses Kapitels umfassen vier Bereiche:

- die Organisation der Telearbeit,
- die Telearbeitsrechner der TelearbeiterInnen,

- die Kommunikationsverbindung zwischen Telearbeitsrechnern und Organisation bzw. Institution (zumeist außerhalb der Räumlichkeiten der Organisation bzw. Institution) und
- den Kommunikationsrechner der Institution zur Anbindung des Telearbeitsrechners (zumeist innerhalb der Räumlichkeiten der Organisation bzw. Institution).

Die in diesem Kapitel aufgeführten Maßnahmenempfehlungen konzentrieren sich auf zusätzliche Sicherheitsanforderungen, die sich aus einem Einsatz eines IT-Systems im Bereich der Telearbeit ergeben. Alle übrigen für dieses IT-System erforderlichen organisatorischen, personellen und technischen Sicherheitsmaßnahmen sind selbstverständlich ebenfalls vollinhaltlich zur Anwendung zu bringen.

6.3.1 Mobile IT-Geräte

Unter mobilen IT-Geräten sind alle für einen transportablen Einsatz geeigneten Geräte zu verstehen, so etwa Notebooks, Tablets und Smartphones sowie auch mobile Datenträger wie USB-Festplatten und -Sticks.
Sie sind vielfältigeren Risiken ausgesetzt als stationäre Geräte sowie als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Die meisten Umfeldbedingungen bei mobilem Einsatz liegen zumeist außerhalb der direkten Einflussnahme der BenutzerInnen, daher müssen sie für möglichst sichere Aufbewahrung mobiler IT-Geräte auch außer Haus sorgen.
Immerhin gibt es eine Vielzahl von Möglichkeiten, mobile IT-Systeme unterwegs zu schützen. Damit diese Möglichkeiten auch zum Einsatz kommen, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die BenutzerInnen ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von mobilen IT-Systemen erstellt werden.

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten MitarbeiterInnen für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Da es bei mobilen IT-Systemen eine große Bandbreite von Varianten und Kombinationsmöglichkeiten für unterschiedliche Hardware sowie für Software gibt, sollten sie vor allem über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden.

Die MitarbeiterInnen sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und dies unterwegs auch nicht in Hör- und Sichtweite von Externen machen sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden.

Ebenso sind bei der Nutzung von mobilen IT-Systemen diverse Punkte zu regeln:

- Die BenutzerInnen müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um Einschränkungen den BenuzerInnen transparent zu machen. Dienstgeheimnisse dürfen nur dann auf mobilen IT-Systemen verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- Für Daten, die ein hohes Maß an Sicherheit verlangen (z. B. Angebote, Konstruktionsdaten, Wirtschaftsdaten des Unternehmens, personenbezogene oder sensible Daten) ist die Installation eines Zugriffsschutzes (über Passwort oder Chipkarte) unabdingbar sowie einer Festplatten-, Container- oder Dateiverschlüsselung dringend zu empfehlen. Hierfür gibt es eine Reihe von brauchbaren Produkten zur transparenten Laufwerks- oder Containerverschlüsselung.
- Dabei ist zu beachten, dass die Zulässigkeit von Verschlüsselungstechnologien in den einzelnen Staaten unterschiedlich geregelt ist. Besondere Gegebenheiten können sich in verschiedenen Zielgebieten und in speziellen Situationen (etwa bei einer besonders eingehenden Zollkontrolle) ergeben, etwa dass bestimmte Verschlüsselungsprodukte nicht (auch nicht in installierter Form) importiert werden dürfen oder die verschlüsselten Daten den Zollbeamten offengelegt werden müssen. Bei Mitnahme mobiler IT Geräte auf Auslandsreisen ist dies bereits im Vorfeld zu klären. Eine mögliche Alternative zu mitgenommenen Daten wären etwa zugriffsgeschützte Online-Festplatten (Cloud-Speicher) am Server der eigenen Organisation.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile MitarbeiterInnen von unterwegs Zugriff auf interne Daten ihrer Institution erhalten sollen. Falls dies vorgesehen ist, muss dieser Zugriff angemessen geschützt werden
- Es muss geklärt werden, ob diese auch für private Zwecke benutzt werden dürfen, beispielsweise für private Schreiben oder gar Spiele nach Feierabend. Insbesondere muss damit gerechnet werden, dass bei privater Nutzung eines Internetzugangs weniger sichere Seiten aufgerufen werden als für dienstliche Zwecke.
- Die BenutzerInnen sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen sollte klar geregelt werden. Keinesfalls dürfen solche Geräte ohne ausdrückliche Zustimmung der Organisation Dritten zur Reparatur oder Softwarewartung übergeben werden oder unautorisiert darauf irgendwelche Software installiert werden.

- Bei jedem Wechsel der BesitzerInnen müssen alle benötigten Zugangsmechanismen (z. B. Passwörter) gesichert weitergegeben werden.

Ein mobiles IT-System stellt einen Wert dar, der potenzielle Diebe anlocken könnte. Dies gilt besonders für fremde Räumlichkeiten wie Hotelzimmer sowie für Kraftfahrzeuge. Daher sollten mobile IT-Systeme möglichst nicht unbeaufsichtigt bleiben oder ungeschützt herumliegen, sondern in einem Schrank bzw. im Kofferraum eingeschlossen sein. Ist das nicht möglich, sollten sie zumindest verdeckt werden, damit sie von außen nicht sichtbar sind. Alle Schutzmechanismen müssen aktiviert sein, wenn sich die Geräte nicht unmittelbar bei den BesitzerInnen befinden.

Für die Nutzung zu Hause (Telearbeit/Homeoffice) bieten einige Geräte zusätzlich die Möglichkeit zum Anketten des Gerätes. Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.

Werden mobile IT-Systeme in fremde Büroräume mitgenommen, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten. Es kann aber auch sein, dass sie gar nicht mitgenommen werden dürfen, sondern etwa beim Portier abgegeben werden müssen. In solchen Fällen sind die Geräte auszuschalten, um unkontrollierte Nutzung zu verhindern.

Wird ein mobiles IT-Gerät in fremden Büroräumen benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das Gerät ausgeschaltet werden.

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von mobilen IT-Systemen in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. für Besprechungsräume sinnvoll sein, da die Gefahr des bewussten oder unbewussten Abhörens der Raumgespräche über Mobiltelefone besteht.

Allerdings wird ein solches Verbot zunehmend schwieriger durchsetzbar, da Notebooks und Mobiltelefone immer mehr zu unverzichtbaren Arbeitsmitteln in Meetings - gerade auch mit hochrangigen Besetzungen - geworden sind. Da die Geräte immer kleiner werden, wird auch die Kontrolle zunehmend schwieriger.

Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass mobile IT-Systeme mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

6.3.1.1 Laptop, Notebook, Tablet

Darunter versteht man Computer, die aufgrund ihrer Bauart transportfreundlich sind und mobil nutzbar sind. Auch eine stationäre Nutzung solcher mobiler Geräte ist möglich. Ein Notebook hat eine kompaktere Bauform als ein Arbeitsplatzrechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Es verfügt über eine Festplatte/SSD und manchmal auch noch über weitere Speichergeräte wie DVD- oder Blu-ray-Laufwerke sowie oft über Schnittstellen zur Kommunikation über verschiedene Medien (beispielsweise LAN, USB, Thunderbolt, WLAN). Notebooks können mit allen üblichen Betriebssystemen wie Windows, MacOS oder Linux betrieben werden.

Typischerweise wird ein Notebook zeitweise allein, ohne Anschluss an ein Rechnernetz, betrieben und von Zeit zu Zeit wird es zum Abgleich der Daten sowie zur Datensicherung mit dem Behörden- oder Unternehmensnetz verbunden. Häufig wird es auch während der mobilen Nutzung über WLAN oder Mobilfunk direkt mit externen Netzen, insbesondere mit dem Internet, verbunden, so dass es indirekt als Brücke zwischen dem LAN und dem Internet wirken kann.

Typische Gefährdungen für Notebooks

- Beeinträchtigungen durch wechselnde Einsatzumgebungen,
- Umwelteinflüsse (Nässe, Kälte, Hitze, Vibrationen),
- Verlust, Diebstahl,
- Fahrlässige Zerstörung von Gerät oder Daten,
- Manipulation oder Zerstörung von Geräten oder Zubehör,
- Gefährdung durch Reinigungs- oder Fremdpersonal,
- Unerlaubte Ausübung von Rechten,
- Unkontrollierter Einsatz von Datenträgern,
- Unerlaubte Installation von Software,
- Ungeordneter oder unerlaubter Benutzerwechsel,
- Ausfall der internen Stromversorgung,
- Verlust gespeicherter Daten,
- Informationsverlust bei erschöpftem Speichermedium,
- Softwareschwachstellen oder -fehler,
- Nichtbeachtung von Sicherheitsmaßnahmen,
- Unzureichender Umgang mit Passwörtern oder anderen Authentifizierungskomponenten,
- Fehlerhafte Nutzung, Konfigurations- und Bedienungsfehler, Fehler bei der Synchronisation,
- Sorglosigkeit im Umgang mit Informationen,
- Manipulation an Informationen oder Software,

- Schadprogramme, Trojanische Pferde, Viren,
- Vertraulichkeitsverlust schützenswerter Informationen,
- Unberechtigte Privatnutzung,
- Unberechtigte Datenweitergabe,
- Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Maßnahmenempfehlungen für Notebooks

Im Rahmen des Einsatzes von Notebooks sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1. Richtlinien für die Nutzung von Notebooks:
   Um Notebooks sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht. Darauf aufbauend ist die Notebook-Nutzung zu regeln und Sicherheitsrichtlinien dafür zu erarbeiten. Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und ob und in welcher Weise ein Anschluss an das Unternehmens- bzw. Behördennetz gestattet wird. Ebenso ist zu regeln, ob und in welcher Form bei mobiler Nutzung eine direkte Verbindung des Notebooks mit dem Internet zulässig ist.
2. Beschaffung von Notebooks:
   Für die sichere Beschaffung von Notebooks müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden
3. Sichere Installation von Notebooks:
   Eine sorgfältige Auswahl der Betriebssystem- und Softwarekomponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der Notebooks auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem zu realisieren. Dabei ist der Einsatz von Verschlüsselungsprodukten für tragbare IT-Systeme von besonderer Bedeutung, da bei Notebooks ein relativ hohes Diebstahlsrisiko besteht und die normalen Funktionen der Zugangs- und Zugriffskontrolle ihre Wirksamkeit verlieren, wenn das Notebook unter der Kontrolle des Diebes steht. Zugleich sind allfällige Einfuhrbeschränkungen für Verschlüsselungsprodukte oder verschlüsselte Daten bei Auslandsreisen zu beachten.
4. Sichere Konfiguration der installierten Komponenten:
   Je nach Sicherheitsanforderungen müssen die beteiligten Softwarekomponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig vom eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch

hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer BenutzerInnen erforderlich ist. Notwendig ist auch die Änderung voreingestellter Passwörter, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.

5. Sicherer Betrieb von Notebooks:
   Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Notebooks ist die Installation und permanente Aktualisierung eines Virenschutzprogramms. Notebooks werden häufig über längere Zeit losgelöst vom Firmen- oder Behördennetz oder auch mit temporären Verbindungen zum Internet betrieben. Somit sind unter Umständen einerseits ihre Virendefinitionsdateien veraltet und sie sind andererseits einem hohen Infektionsrisiko ausgesetzt. Schutz vor Schadprogrammen und Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen sind daher für Notebooks ganz besonders wichtig. Diese Geräte können sonst bei Anschluss an ein Firmen- oder Behördennetz Infektionsquellen ersten Grades darstellen. Sofern Notebooks bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht allein nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Notebooks auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Soll ein Notebook, das mit direktem Internetzugang betrieben wurde, wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieses Notebook nicht mit Schadsoftware infiziert ist. Erst wenn dies sichergestellt ist, darf der Anschluss an das lokale Netz erfolgen. Dies gilt auch für den Fall, dass der Anschluss an das Unternehmens- bzw. Behördennetz über ein Virtual Private Network (VPN) erfolgt, da Viren auch über verschlüsselte Kommunikationsverbindungen weiterverbreitet werden können.
   Bei einem Wechsel zwischen netzgebundenem und mobilem Betrieb müssen die Datenbestände zwischen dem Server und dem Notebook synchronisiert werden. Es muss dabei gewährleistet werden, dass jederzeit erkennbar ist, ob sich die aktuellste Version der bearbeiteten Daten auf dem Notebook oder im Netz befindet.
   Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei Notebooks vor allem organisatorische Maßnahmen (Hard- und Softwaremanagement) notwendig. Um einen Überblick über die aktuell in das lokale Netz eingebundenen Notebooks zu behalten und die Konfiguration aller Notebooks jederzeit nachvollziehen zu können, ist eine zentrale Verwaltung dieser Geräte wichtig. Weitere spezifische Maßnahmen für Einzelsysteme betreffen vor allem den Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern sowie die Verwendung von Sicherheitsfunktionen (vgl. 9.6.3 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen). Je nach der in einem Gebäude oder

Büroraum gegebenen physischen Sicherheit kann es auch sinnvoll oder sogar notwendig sein, Diebstahlsicherungen vorzusehen. Bei mobiler Nutzung ist in jedem Fall für geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz zu sorgen, um das Notebook vor Diebstahl zu schützen.

6. Aussonderung:
   Bei Übergabe von Notebooks an andere BenutzerInnen, sei es im Rahmen des normalen Betriebs oder auch bei ihrer Aussonderung, ist darauf zu achten, dass keine schützenswerten Informationen mehr auf der Festplatte vorhanden sind. Gegebenenfalls ist dazu auch eine Neuinstallation der Software durchzuführen.
7. Datensicherung von Notebooks:
   Die Vorgehensweise und der erforderliche Umfang der Datensicherung richten sich nach dem Einsatzszenario des Notebooks.

Nicht zuletzt sollte darauf geachtet werden, für Reisen bzw. längerem Einsatz unterwegs das Ladegerät sowie ggf. Adapter für andere Stromspannungen bzw. Steckdosen im Ausland mitzuführen.

[Quelle: BSI SYS.3.1]

6.3.1.2 Mobiltelefon, Smartphone

Mobiltelefone sind inzwischen nicht mehr wegzudenkende Bestandteile der Kommunikationsinfrastruktur geworden und stellen in ihrer modernsten Ausprägung als Smartphone bereits die Funktionalität von Laptop, Notebook, Tablet zur Verfügung - und schaffen damit zusätzlich auch deren Sicherheitsrisiken. Hier wird auf die typischen Eigenschaften der Mobilfunkkomponente eingegangen.

Ein Mobiltelefon besteht aus dem Mobilfunkgerät selbst und dem Identifikationsmodul, der SIM-Karte (SIM - Subscriber Identity Module bzw. eSIM – embedded SIM). Damit kann zwischen BenutzerInnen und Gerät unterschieden werden. Das Mobilfunkgerät ist gekennzeichnet durch seine international eindeutige Seriennummer (IMEI - International Mobile Equipment Identity). Manche Mobilfunkgeräte verfügen über zwei IMEI-Nummern (z.B. IMEI, IMEI2). Die BenutzerInnen werden durch ihre auf der SIM-Karte gespeicherten Kundennummer (IMSI - International Mobile Subscriber Identity) identifiziert. Sie wird dem Teilnehmer beim Vertragsabschluss vom Netzbetreiber zugeteilt und ist von den Telefonnummern zu unterscheiden. Damit ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobilfunkgeräte nutzen kann.

Auf der SIM-Karte wird u. a. die Rufnummer gespeichert und die kryptographischen Algorithmen für die Authentisierung und Nutzdatenverschlüsselung implementiert. Darüber hinaus können dort Kurznachrichten, Gebühreninformationen, ein persönliches Telefonbuch und weitere Daten gespeichert werden.

Es muss beachtet werden, dass der Netzbetreiber eine Reihe von Zugriffsmöglichkeiten auf das Telefon bzw. die SIM-Karte hat und auch nutzt, vom „SIM-Toolkit“ zum Herunterladen neuer Funktionen bis zum Speichern aller möglicher Daten:

- wo sich der Teilnehmer befindet und ob er sein Mobiltelefon eingeschaltet hat,
- ob der Teilnehmer überhaupt berechtigt ist, das Mobilfunknetz zu nutzen (Identifikationsregister),
- ob das verwendete Gerät im Netz zugelassen ist,
- welche Geräte als defekt oder als gestohlen gemeldet sind (graue bzw. schwarze Listen),
- Verbindungsdaten für die Abrechnung der Dienste, aber auch auf Grund einer Anforderung der Strafverfolgung und Terrorismusbekämpfung. Sie enthalten Angaben über Kommunikationspartner (z. B. Rufnummern der Angerufenen), Zeitpunkt und Dauer der Verbindungen und die Standorte. Mobiltelefone können also durchaus sensitiv sein.

Die kryptographischen Algorithmen der SIM-Karte dienen zur Identifikation des Teilnehmers gegenüber dem Netzbetreiber und zur Verschlüsselung der Gesprächs- bzw. Übertragungsinhalte. Es handelt sich aber nicht um End-to-End-Verschlüsselung bis zu den Kommunikationspartnern: auf dem Weg werden üblicherweise auch Festnetzstrecken genutzt, wo keine Verschlüsselung wirksam ist.

Typische Gefährdungen für Mobiltelefone

- Unzureichende Planung bei der sicheren Anschaffung von Mobiltelefonen
- Umwelteinflüsse (Nässe, Kälte, Hitze)
- Verlust, Diebstahl
- Fehlerhafte Bedienung und Verwendung
- Fahrlässige Zerstörung von Gerät oder Daten
- Manipulation oder Zerstörung von Geräten oder Zubehör
- Unerlaubte Ausübung von Rechten
- Unkontrollierter Einsatz von Datenträgern (z. B. Speicherkarten)
- Unerlaubte Installation von Software (z. B. Apps)
- Ungeordneter oder unerlaubter Benutzerwechsel
- Ausfall des Geräts, der Stromversorgung oder der Internetverbindung
- Nichtverfügbarkeit des Mobilfunknetzes
- Verlust gespeicherter Daten bzw. des Mobiltelefons
- Informationsverlust bei erschöpftem Speichermedium
- Softwareschwachstellen oder -fehler
- Nichtbeachtung von Sicherheitsmaßnahmen
- Unzureichender Umgang mit Passwörtern

- Fehlerhafte Nutzung, Konfigurations- und Bedienungsfehler, Fehler bei der Synchronisation
- Manipulation an Informationen oder Software (z. B. unerlaubtes Akzeptieren fremder SIM-Karten)
- Sorglosigkeit im Umgang mit Informationen
- Phishing Attacken auf Passwörter oder PINs via SMS
- Schadprogramme, Trojanische Pferde, Viren
- Vertraulichkeitsverlust schützenswerter Informationen
- Unzureichende Identifikationsprüfung von Kommunikationspartnern
- Unberechtigte Privatnutzung
- Unberechtigte Datenweitergabe
- Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
- Abhören von Raumgesprächen bzw. Videokonferenzen mit Mobiltelefonen
- Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
- Einsatz veralteter Mobiltelefone (z.B. Hardware, Software)
- Versehentliche Preisgabe von Informationen
- Übergreifende Wirkung bei Sicherheitsvorfällen (z.B. Aushebeln von Mehrfaktorauthentifizierung via kompromittiertem Smartphone)

Die folgenden Anforderungen zur Einrichtung mobiler Geräte müssen erfüllt werden:

- Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
- Sperrmaßnahmen bei Verlust eines Mobiltelefons
- Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen
- Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und darin verwendeter Speicherkarten

Maßnahmenempfehlungen für Mobiltelefone

Für Mobiltelefone bzw. Smartphones sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Nutzung bis zur Notfallvorsorge:

1. Planung und Konzeption:
   Damit die Möglichkeiten, Mobiltelefone sicher einzusetzen, in der Praxis auch tatsächlich genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, die die umzusetzenden Maßnahmen beschreibt.
2. Beschaffung:
   Bei häufiger und wechselnder dienstlicher Nutzung von Mobiltelefonen, die vom Unternehmen oder der Behörde zur Verfügung gestellt werden, kann es sinnvoll sein, diese Telefone in einer Sammelaufbewahrung zu halten.
3. Betrieb:

Zum sicheren Betrieb von Mobiltelefonen gehören unter anderem die Sicherstellung der Energieversorgung und bei Bedarf auch der Schutz vor Rufnummernermittlung. Falls das Gerät zur Datenübertragung eingesetzt wird, sind zur zuverlässigen Funktionsweise und zum Schutz gegen Missbrauch zu beachten:

- Kurzmitteilungen (SMS): Damit lassen sich Texte mit maximal 160 Zeichen von einem Mobiltelefon zum anderen oder auch an E-Mail-Adressen senden. Am Mobiltelefon selbst können auch längere Texte eingegeben werden, diese werden aber automatisch in mehrere SMS mit jeweils 160 Zeichen aufgeteilt. Die Übertragung von Kurzmitteilungen erfolgt immer über die Kurzmitteilungszentrale, welche die Nachrichten an den jeweiligen Empfänger weiterleitet. Im Internet gibt es diverse Angebote, über die mit minimalen Kosten Kurzmitteilungen webbasiert versandt werden können.
  Es ist ohne großen Aufwand möglich, auf diese Weise eine große Anzahl von SMS-Nachrichten an ein Mobiltelefon zu senden. Die Auswirkungen von SMS-Spam sind wie bei E-Mail: Die E-Mail-Box bzw. der Speicherplatz reicht nicht aus und ernsthafte Anfragen kommen nicht durch. Darüber hinaus entstehen den BenutzerInnen (evtl. hohe) Kosten (Mehrwert-SMS!). Hiergegen hilft nur, im Vorfeld die eigene Rufnummer nicht zu breit zu streuen, also z. B. auf den Eintrag in Telefonbücher zu verzichten, bzw. im Schadensfall eine Zeit lang auf SMS zu verzichten.
  Eine Identifikation des Absenders ist bei SMS nicht zuverlässig möglich, da sie nur über die Rufnummer des Absenders erfolgt. Beim Versand von Kurzmitteilungen über das Internet erfolgt i. Allg. überhaupt keine eindeutige Identifizierung. Das wird für Phishing-SMS ausgenützt. Je nach Inhalt einer empfangenen Kurzmitteilung ist es sinnvoll nachzufragen, ob diese wirklich vom angegebenen Absender stammt.
  Es passiert immer wieder, dass SMS-Nachrichten beim falschen Empfänger landen, weil eine falsche Rufnummer angegeben oder ein falscher Eintrag aus dem Telefonbuch als Empfänger ausgewählt wurde. Auch wenn die Displays der Mobiltelefone klein sind, sollten die Empfängerangaben vor dem Absenden überprüft werden.
- E-Mail: können über Mobiltelefone empfangen und verschickt werden. Die potenziellen Sicherheitsprobleme und Maßnahmen sind die gleichen wie bei auf PC üblicher Nutzung von E-Mail. Zusätzlich treten durch die geringere Displaygröße und die Art der Bedienung der Geräte weitere Probleme auf. So sind zum Beispiel das Ziel von in E-Mails enthaltenen Links sowie Domains von aufgerufenen Webseiten schwieriger zu erkennen. Sicherheitsmaßnahmen wie Verschlüsselung oder Signatur sind hierbei möglich, jedoch standardmäßig nicht aktiv oder nur durch zusätzliche Apps möglich.

- Kommunikation: Telefongespräche aber auch andere Übertragungskanäle (E-Mail, Messenger-Applikationen, plattformübergreifende Dateiaustauschprogramme, …) sind anfällig für Betrugsformen wie zum Beispiel falsche Support-Angebote, Phishing oder auch CEO-Fraud, bei dem sich jemand als Vorgesetzter oder sonstige Autoritätsperson ausgibt und Forderungen stellt, meist unter Vorwand einer zeitlichen Dringlichkeit oder Vertraulichkeit. Direkte Rückfragen sind bei Telearbeit in so einem Fall schwieriger bzw. seltener. Daher ist es wichtig Mitarbeiterinnen und Mitarbeiter entsprechend zu schulen und Vorgehensweisen für solche Fälle zu definieren (z.B. Rückfrage über anderen Kanal, etwa per direkter Telefonnummer falls Forderung per E-Mail eingelangt ist).
- Kopplung zu anderen IT-Systemen: Diese kann über NFC, USB, WLAN, Infrarot (IrDA - Infrared Data Association) oder Bluetooth erfolgen. Es ist zu beachten, dass bei Funkschnittstellen ein Abhörrisiko besteht, und sich mobile Geräte oft automatisch untereinander verbinden, ohne dass dies besonders auffällt (bei Windows-PCs wird meist ein kleines Icon in der Task-Leiste angezeigt).
- Herunterladen von Software oder Daten aus dem Internet (Apps, Klingeltöne, Themes oder Ähnliches) sollte bei dienstlich genutzten Mobiltelefonen unterbunden oder verboten werden. Eine Auswahl erlaubter Apps kann vordefiniert werden. Von Apps gehen diverse Gefahren aus, die je nach Berechtigungen variieren, wobei vor allem Überwachung oder Diebstahl sensibler Daten zu beachten sind.
- Mobiltelefone sind in der Regel mit dem Internet verbunden. Erfolgt diese Internetverbindung gleichzeitig mit einer Kopplung an eine IT-Komponente der Organisation im Netzwerk, dann entsteht *eine unkontrollierbare Verbindung vom Netzwerk in die Außenwelt unter Umgehung des Firewall-Schutzes!* Dafür ist entsprechende Sensibilisierung zu schaffen. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen.
- Deaktivieren nicht erforderlicher Drahtlosverbindungen: Jede drahtlose Schnittstelle (z.B. IrDA, Bluetooth, WLAN) sollte nur dann aktiviert werden, wenn die Verwendung notwendig ist. Ist die Verwendung nicht mehr erforderlich, sollten diese Schnittstellen umgehend deaktiviert werden.
- Aktivieren von Sicherheitsprogrammen.

4. Notfallvorsorge: Ein Mobiltelefon kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn es dringend benötigt wird oder dadurch wichtige Daten verloren gehen.

    - Die wichtigsten Einstellungen wie PINs und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihres Schutzbedarfs sicher aufbewahrt werden.

- Alle auf der SIM-Karte oder im Telefon gespeicherten Daten sollten über SIM-Kartenleser bzw. entsprechende (Backup-)Software - unter Wahrung der Regelungen für die Datenübertragung - in einen PC eingelesen und dort verwaltet werden. Damit kann Datensicherung sowie Synchronisation (ggf. auch mehrerer Mobiltelefone) durchgeführt werden. Die IMEI/MEID-Nummer sollte für den Fall des Verlusts oder Diebstahls notiert bzw. gespeichert werden. Die Nummer kann im Eingabefeld für Telefonanrufe durch wählen von **#06#* abgefragt werden. Dual-SIM-Handys besitzen zwei IMEI-Nummern.
- Der Ladezustand und die Funktionsfähigkeit des Mobiltelefon-Akkus sollten regelmäßig überprüft werden.
- Wenn ein Mobiltelefon kontinuierlich verfügbar sein soll, sollte ein Ersatz-Mobiltelefon, mindestens aber ein Ersatz-Akku (sofern der Akku einfach austauschbar ist) bzw. eine Powerbank mitgeführt werden. Das ist etwa dann unabdingbar, wenn Mobiltelefone im Rahmen von Alarmierungen eingesetzt werden (z. B. die Einbruchmeldeanlage setzt Alarmmeldungen über Mobilfunk ab oder Notfallpersonal wird über Mobiltelefone benachrichtigt).

5. Reparatur: sollte nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

    - Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei der Auswahl des Mobiltelefons bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.
    - Bevor das Mobiltelefon zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. der Anrufspeicher, gespeicherte E-Mails und das Telefonbuch im Gerät gelöscht werden, soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollte die SIM-Karte entfernt werden. Bei unverschlüsselten Geräten reicht das einfache Löschen von Dateien nicht aus, hierbei muss der Speicherplatz nach dem Löschen noch überschrieben werden, beispielsweise durch Aufnahme eines Videos bis der gesamte Speicherplatz voll ist. Alternativ kann eine sichere Löschung auch durch entsprechende Software durchgeführt werden. Bei verschlüsselten Geräten reicht eine Rücksetzung auf den Werkszustand, wodurch auch ein neuer Schlüssel für die Speicherverschlüsselung generiert und der alte Schlüssel gelöscht wird.

6. Verlust, Diebstahl: die SIM-Karte dieses Telefons sollte unverzüglich gesperrt werden, um Missbrauch und unnötige Kosten zu verhindern. Bei eSIM ist neben einer Sperre bei manchen Anbietern auch ein Austausch des eSIM-Profils möglich. Der Verlust oder Diebstahl sollte bei der Polizei angezeigt werden und dabei auch die IMEI-Nummer angegeben werden. Mit dieser ist unter

Umständen ein Auffinden des Gerätes möglich. Smartphones bieten weitere Möglichkeiten zur Ortung und Wiedererlangung aber auch zur Sperrung oder Fernlöschung des Geräts über betriebssystemeigene oder zusätzliche Apps. Dabei müssen jedoch Datenschutzaspekte abgewogen werden.

7. Aussonderung und Entsorgung: Mobiltelefone sollten jedenfalls ordnungsgemäß ausgesondert bzw. entsorgt werden. Das bedeutet, eine Wiederherstellung auf den Werkszustand ist notwendig und demzufolge eine Entfernung aller Daten. Das gilt insbesondere für die Entfernung sensibler Daten. Eventuell enthaltene entnehmbare Speicherkarten (z.B. SD-Karten) sollten ebenfalls in gesicherter Form ausgesondert bzw. entsorgt werden.
8. Awareness: Eine Sensibilisierung der Mitarbeiterinnen bzw. Mitarbeiter über die Bedrohungen in Verbindung im allgemeinen Umgang und mit der Nutzung von Mobiltelefonen sollte forciert werden. Dies fordert einerseits Sensibilisierung über die Verwendung der integrierten Sicherheitsfunktionen (z.B. Sperrcode, PIN für SIM-Karte, Verschlüsselung, VPN) aber auch andererseits eine Sensibilisierung welche Prozesse im Verlustfall oder bei Diebstahl einzuhalten sind.

Nicht zuletzt sollte darauf geachtet werden, für Reisen bzw. längeren Einsatz unterwegs das Ladegerät sowie ggf. Adapter für andere Stromspannungen bzw. Steckdosen im Ausland mitzuführen.

[Quelle: BSI SYS.3.3, INF.9]

6.3.1.3 Wechselmedien und externe Datenspeicher (USB-Sticks, -Platten, SD-Karten, DVDs, BDs)

Handelsübliche PCs sind heute zum Teil mit CD-/DVD-ROM-Laufwerk, CD-/DVD-Writer bzw. Blu-ray(BD)-Laufwerk ausgestattet. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen, die von neueren Betriebssystemen automatisch erkannt werden. Beispiele sind USB-Memory-Sticks bzw. Festplatten/SSDs, die in die USB-Schnittstelle gesteckt werden, und SD-Karten.

Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich potenzielle Sicherheitsprobleme:

- Der PC könnte von solchen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software (auch Schadsoftware, Viren, Trojanische Pferde) von solchen Laufwerken eingespielt werden.
- Dienstliche Daten könnten unberechtigt auf Wechselmedien kopiert werden.
- Verlust oder Diebstahl der Wechselmedien führt zur Kompromittierung der darauf gespeicherten (z.B. schützenswerten) Daten.
- Defekte Schnittstellen bzw. Wechselmedien führen zu Datenverlust.

Beim Booten von Wechselmedien oder beim Installieren von Fremdsoftware können nicht nur Sicherheitseinstellungen außer Kraft gesetzt werden, sondern der PC kann auch mit Computerviren und anderen Schadprogrammen infiziert werden.

Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- Sensibilisierung zum sicheren Umgang mit Wechselmedien und zu Verlust- sowie Manipulationsmeldungen:
  Aufbau des Bewusstseins über den erlaubten sicheren Umgang mit Wechselmedien sowie in diesem Zusammenhang notwendiger Einschränkungen. Bei zumindest dem Verdacht auf eine Manipulation bzw. dem Verlust eines Wechselmediums ist eine geeignete Meldung durchzuführen. Diese Meldung sollte Angaben zu den darauf gespeicherten Daten enthalten und den dafür vorgesehenen Meldeweg einhalten.
- Ausbau von Laufwerken:
  Der Ausbau der Laufwerke für Wechselmedien (bzw. der Verzicht bei der Beschaffung) bietet zwar den best-möglichen Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Weiters ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert. Diese Lösung sollte in Betracht gezogen werden, wenn ein höherer Schutzbedarf bzw. besondere Sicherheitsanforderungen bestehen.
- Physischer Verschluss bzw. Versperren von Laufwerken:
  Für einige Laufwerksarten gibt es abschließbare Einschubvorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann (z.B. für USB). Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Außerdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden. Nachteilig sind die Beschaffungskosten für die Laufwerksschlösser und der Aufwand für die erforderliche Schlüsselverwaltung. Daher ist diese Lösung nur bei höherem Schutzbedarf oder besonderen Sicherheitsanforderungen sinnvoll.
- Deaktivierung im BIOS/UEFI bzw. Betriebssystem:
  Im BIOS bzw. UEFI bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwortschutz der BIOS-Einstellungen kann dadurch das unkontrollierte Booten von Wechselmedien und mobilen Datenträgern unterbunden werden. Weiters können die vorhandenen Laufwerke und Schnittstellen bei modernen Betriebssystemen einzeln deaktiviert werden. Dies erschwert die unberechtigte Nutzung, z. B. die Installation von Fremdsoftware oder das Kopieren auf Wechselmedien. Die Deaktivierung der Laufwerke im BIOS bzw. Betriebssystem hat den Vorteil, dass keine Hardwareänderungen erforderlich sind. Die

entsprechenden Einstellungen im Betriebssystem können gegebenenfalls sogar zentral vorgenommen werden. Damit diese Vorgehensweise wirksam ist, muss sichergestellt sein, dass die BenutzerInnen nicht über die Berechtigungen im Betriebssystem verfügen, um die Deaktivierung der Laufwerke rückgängig zu machen.

- Kontrolle der Schnittstellennutzung:
  Der Betrieb von externen Speichermedien wie USB-Memory-Sticks lässt sich nur sehr schwer verhindern, wenn die verwendete Schnittstelle auch für andere (erlaubte) Zusatzgeräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Dadurch ist es in der Regel nicht sinnvoll, ein „USB-Schloss“ zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren. Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Bei einigen Zusatzprogrammen zur Absicherung der USB-Schnittstellen kann zusätzlich festgelegt werden, ob von externen Datenträgern nur gelesen werden kann. Alternativ kann das Hinzufügen von Geräten überwacht werden. Beim Anschluss von Datenträgern an externen Schnittstellen werden oft vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Einzelheiten sind produkt- und betriebssystemspezifisch.
- Verschlüsselung und Integritätsschutz:
  Es gibt Produkte, die dafür sorgen, dass ausschließlich Zugriffe auf dafür zugelassene mobile Datenträger möglich sind. Eine Lösung ist beispielsweise, dass nur noch mobile Datenträger gelesen und beschrieben werden können, die mit bestimmten kryptographischen Verfahren bzw. Schlüsseln verschlüsselt worden sind. Dies schützt nicht nur vor unbefugtem Zugriff über manipulierte mobile Datenträger, sondern schützt auch die Daten auf den mobilen Datenträgern bei Verlust oder Diebstahl. Neben der Verschlüsselung sollten Verfahren zum Schutz gegen vorsätzliche bzw. unabsichtliche Veränderungen der gespeicherten Daten angewendet werden (z.B. Checksummen, digitale Signaturen, Hashwerte).
- Richtlinien für die Nutzung:
  In vielen Fällen dürfen die BenutzerInnen die eingebauten Laufwerke für Wechselmedien oder Speichermedien an externen Schnittstellen durchaus verwenden, die Nutzung ist jedoch durch entsprechende Richtlinien reglementiert. Auf technischer Ebene sollte dann lediglich das Booten von Wechselmedien im BIOS bzw. UEFI deaktiviert werden. Ausbau, Verschluss oder Deaktivierung der Laufwerke im Betriebssystem kommen nicht in Frage. In diesem Fall sollten die Richtlinien für die Nutzung der Laufwerke und Speichermedien so explizit wie möglich definiert werden. Beispielsweise kann ein generelles Verbot ausgesprochen werden, nur das Kopieren öffentlicher Text-Dokumente wird erlaubt. Die Richtlinien müssen allen BenutzerInnen bekannt gemacht und die Einhaltung kontrolliert werden. Die Installation und das Starten von Programmen, die von Wechselmedien eingespielt wurden,

sollte untersagt und so weit wie möglich auch technisch unterbunden werden (siehe auch 14.3.1 Nutzungsverbot nicht freigegebener Software). Darüber hinaus sollte die Mitnahme von Wechselmedien bzw. Speichermedien von einer solchen Richtlinie abgedeckt sein. Diese rein organisatorische Lösung sollte nur dann gewählt werden, wenn die BenutzerInnen hin und wieder oder regelmäßig auf die Laufwerke zugreifen müssen. Anderenfalls sollte der Zugriff - wie oben beschrieben - durch technische Maßnahmen unterbunden werden.

Bei der Auswahl einer geeigneten Vorgehensweise müssen immer alle Laufwerke für Wechselmedien berücksichtigt werden, aber ebenso auch alle Möglichkeiten, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internetanbindungen. Wenn der PC über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen. Besonderes Augenmerk ist auf den Schutz vor Schadprogrammen, z. B. Computerviren oder „Trojanische Pferde“, zu richten.

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die BenutzerInnen über die Gefährdung durch Laufwerke für Wechselmedien informiert und sensibilisiert werden.

[Quelle: BSI SYS.4.5]

6.3.2 Geeignete Einrichtung eines mobilen Arbeitsplatzes

Die wechselnde Arbeitsumgebung mobiler Arbeitsplätze sollte in geeigneter Form berücksichtigt werden, um die verarbeiteten sowie gespeicherten Daten angemessen zu schützen. In diesem Zusammenhang kann nicht von einer sicheren IT-Infrastruktur ausgegangen werden.

Mobile Arbeitsplätze (z.B. “Coworking Space”, auf Reisen, in Verkehrsmitteln wie etwa Zügen oder bei Kundinnen bzw. Kunden) sind an beinahe allen Plätzen bzw. Orten mit ausreichender Internetverbindung, sowie bei Bedarf notwendiger Energieversorgung, denkbar. Demzufolge kann der Arbeitsplatz in häufigen Abständen sowie zwischen verschiedenen Arbeitsumgebungen wechseln.

Die Einrichtung eines mobilen Arbeitsplatzes muss die folgenden Anforderungen zum Schutz der Informationen erfüllen und setzt dafür notwendige Regelungen voraus:

- Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
- Regelungen für mobile Arbeitsplätze
- Zutritts- und Zugriffsschutz
- Arbeiten mit fremden IT-Systemen

Darüber hinaus sollte ein mobiler Arbeitsplatz die folgenden Anforderungen erfüllen:

- Zeitnahe Verlustmeldung
- Entsorgung von vertraulichen Informationen
- Rechtliche Rahmenbedingungen für das mobile Arbeiten
- Sicherheitsrichtlinie für mobile Arbeitsplätze
- Verschlüsselung tragbarer IT-Systeme und Datenträger
- Nutzung eines Bildschirmschutzes

Bei erhöhtem Schutzbedarf sollte ein mobiler Arbeitsplatz zusätzlich noch die folgenden Anforderungen erfüllen:

- Einsatz von Diebstahlsicherungen
- Verbot der Nutzung unsicherer Umgebungen

[Quelle: BSI INF.9]

6.3.3 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

Der häusliche Arbeitsplatz (Homeoffice) sollte von der übrigen Wohnung zumindest durch eine Tür abgetrennt sein und ausschließlich der beruflichen Tätigkeit dienen.

Der häusliche Arbeitsplatz befindet sich außerhalb der Organisation. Daher sind auch Mitarbeiterinnen bzw. Mitarbeiter im Hinblick auf IT-Sicherheit gefordert. Typische Gefährdungen an häuslichen Arbeitsplätzen sind:

- Fehlende oder unzureichende Regelungen für den häuslichen Arbeitsplatz
- Unbefugter Zutritt zu schutzbedürftigen Räumen des häuslichen Arbeitsplatzes
- Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am häuslichen Arbeitsplatz
- Ungesicherter Akten- und Datenträgertransport
- Ungeeignete Entsorgung der Datenträger und Dokumente
- Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am häuslichen Arbeitsplatz
- Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Die Einrichtung eines häuslichen Arbeitsplatzes sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden. Aus dem Aspekt der IT-Sicherheit entstehen insbesondere folgende zusätzliche Anforderungen:

- Regeln der Rahmenbedingungen zur Verwendung der IT, der Verarbeitung bzw. Speicherung von Daten sowie für die Nutzung von Arbeitsmitteln und zur Entsorgung vertraulicher Informationen am häuslichen Arbeitsplatz

- Sichern dienstlicher Unterlagen
- Transport von Arbeitsmaterial, Datenträgern und Unterlagen
- Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz sowie Einbruchsschutz der an einen angemessenen Schutzbedarf für die örtlichen Gegebenheiten angepasst ist
- Trennung des häuslichen Arbeitsplatzes von privaten Bereichen
- Sichtschutz des Monitors, besonders dann, wenn er durch ein Fenster beobachtet werden könnte
- Überspannungsschutz
- Bereitstellung versperrbarer Behältnisse zur Aufbewahrung von Datenträgern (z.B. für Backups) und Dokumenten sowie bei Bedarf zu deren Vernichtung (z.B. Aktenvernichter)
- Technische Absicherung sowie Einspielen regelmäßiger Software-Aktualisierungen (z.B. Sicherheitspatches) der verwendeten Infrastruktur (z.B. WLAN schützen, Router bzw. Repeater für Meshnetzwerk oder mobile Hotspot via Smartphone sicher einstellen)
- Infrastruktur bei Bedarf redundant aufsetzen sowie verwenden redundant aufgebauter Internetzugänge (z.B. kombinieren von DSL bzw. Kabel in Verbindung mit 4G/5G als Backup)

Dienstlich genutzte IT sollte vom Arbeitgeber bereitgestellt werden, um z. B. per Dienstanweisung ausschließen zu können, dass die IT für private Zwecke benutzt wird.

[Quelle: BSI INF.8]

6.3.4 Regelungen für Telearbeit bzw. Homeoffice

Nach § 2h Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) liegt Arbeit im Homeoffice dann vor, wenn eine Arbeitnehmerin oder ein Arbeitnehmer regelmäßig Arbeitsleistungen in der Wohnung erbringt. Diese Arbeit im Homeoffice ist demzufolge schriftlich zu vereinbaren. Dies kann entweder durch Kollektivverträge bzw. damit verbundener Telearbeitsvereinbarungen, Betriebsvereinbarungen oder zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen TelearbeiterInnen und Arbeitgeber geklärt werden.

Insbesondere sollten folgende Punkte geregelt werden:

- Freiwilligkeit der Teilnahme an der Telearbeit,
- Umfang der Arbeitszeit und Erreichbarkeit sowie Aufteilung der Arbeitszeit zwischen ständiger Betriebsstätte und dem Ort bzw. den Orten der Telearbeit,
- Mehrarbeit und Zuschläge,
- Aufwendungen für Fahrten zwischen Betrieb und häuslicher Wohnung,

- Aufwendungen z. B. für Strom und Heizung,
- Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit),
- Beendigung der Telearbeit.

Am häuslichen Arbeitsplatz sollten zudem dieselben bereits bestehenden Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes (z. B. Einrichtung eines Bildschirmarbeitsplatzes) und der Arbeitsumgebung entweder unverändert oder sinngemäß wie in der Institution gelten. Dies sollte in Absprache mit den TelearbeiterInnen durch den/die in der Institution Verantwortlichen für den Arbeitsschutz, den Datenschutzbeauftragten/CISO sowie dem Betriebs- bzw. Personalrat und den direkten Vorgesetzten der Telearbeiterin bzw. des Telearbeiters begutachtet werden können.

Im Sinne der IT-Sicherheit sollten zusätzlich folgende Punkte behandelt werden:

- Arbeitszeitregelung:
  Die Verteilung der Arbeitszeiten auf Tätigkeiten in der Institution und am häuslichen Arbeitsplatz muss geregelt sein und feste Zeiten über die Erreichbarkeit am häuslichen Arbeitsplatz müssen festgelegt werden.
- Reaktionszeiten:
  Es sollte geregelt werden, in welchen Abständen aktuelle Informationen eingeholt werden (z. B. wie häufig E-Mails gelesen werden) und wie schnell darauf reagiert werden sollte.
- Arbeitsmittel:
  Es kann festgeschrieben werden, welche Arbeitsmittel TelearbeiterInnen einsetzen können und welche nicht genutzt werden dürfen (z. B. nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internetdiensten wird untersagt. Weiters kann die Benutzung von Wechseldatenträgern (Gefahr von Viren) untersagt werden, wenn der Telearbeitsrechner dies nicht erfordert.
- Verwendung digitaler Kollaborationswerkzeuge:
  Die Festlegung zu nutzender digitaler Werkzeuge für die teambasierte Zusammenarbeit (sog. Collaboration Tools) zumeist über große Distanzen sollte vor dem Hintergrund der IT-Sicherheit geregelt werden. Dies umfasst Werkzeuge die dafür geeignet sind, etwa die Bearbeitung von Programmcode, Texten, Tabellen sowie Präsentationen für mehrere Beteiligte zu ermöglichen. Auch decken solche Kollaborationswerkzeuge Programme für die Durchführung von Videokonferenzen (etwa als Alternative zu konventionellen Besprechungen) ab.
- Datensicherung:
  Die TelearbeiterInnen sind zu verpflichten, regelmäßig eine geschützte Datensicherung durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherung bei der Institution zur Unterstützung der Verfügbarkeit sowie zur Vorbeugung vor Datenverlust hinterlegt wird.
- IT-Sicherheitsmaßnahmen:

Die TelearbeiterInnen sind zu verpflichten, die für die Telearbeit notwendigen IT-Sicherheitsmaßnahmen zu beachten und zu realisieren. Die umzusetzenden IT-Sicherheitsmaßnahmen sind den TelearbeiterInnen in schriftlicher Form zu übergeben.

- Datenschutz:
  Die TelearbeiterInnen sind auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.
- Datenkommunikation:
  Es muss festgelegt werden, welche Daten auf welchem Weg übertragen bzw. welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen.
- Transport von Dokumenten und Datenträgern:
  Die Art und Absicherung des Transports zwischen häuslichem Arbeitsplatz und Institution ist zu regeln.
- Meldewege:
  Die TelearbeiterInnen sind zu verpflichten, IT-sicherheitsrelevante Vorkommnisse unverzüglich an eine zu bestimmende Stelle in der Institution zu melden.
- Zutrittsrecht zum häuslichen Arbeitsplatz:
  Für die Durchführung von Kontrollen und für die Verfügbarkeit von Dokumenten und Daten im Vertretungsfall kann ein Zutrittsrecht zum häuslichen Arbeitsplatz (ggf. mit vorheriger Anmeldung) vereinbart werden.

Es empfiehlt sich, diese Regelungen schriftlich festzulegen und sämtlichen TelearbeiterInnen auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

6.3.5 Regelung zur Verwendung digitaler Kollaborationswerkzeuge

Digitale Kollaborationswerkzeuge sind wegen der Arbeit verteilter Teams im Alltag zunehmend relevant. Solche Werkzeuge erlauben die gemeinsame Bearbeitung von Programmcode, Texten, Tabellen sowie Präsentationen durch mehrere Beteiligte aber auch die audiovisuelle Kommunikation über elektronische Videokonferenzsysteme.

Moderne Videokonferenzsysteme mit erweitertem Funktionsumfang zur Darstellung der Online- oder Offline-Aktivitäten für Kommunikation mittels Video, Sprache, Chat oder zum Teilen von Bildschirminhalten, Integration von Kalendern sowie die Möglichkeit Dokumente gleichzeitig zu bearbeiten, wird als Unified Communications & Collaboration (UCC) bezeichnet. Der tatsächliche Funktionsumfang weicht zumeist jedoch je nach ausgewähltem Hersteller ab.

Gefahren bei der Verwendung von Kollaborationswerkzeugen bzw. UCC-Lösungen sind:

- Abhören von Videokonferenzen, Chats oder Telefonaten
- Manipulation der Funktionalität des Systems
- Ungeschützte oder unkontrollierte Kommunikationsendpunkte
- Unzureichend abgesicherte Cloud-Dienste
- Qualitätseinbußen durch unzureichende Dimensionierung
- Fehlerhafte Bedienung bzw. Nutzung
- Automatische bzw. unabsichtliche Annahme von eingehenden Verbindungsanfragen
- Gezieltes Ausspähen von Räumen
- Verlust der Vertraulichkeit durch Kompromittierung von Video-Endpunkten
- Leistungsüberwachung und Profiling
- Kein ordnungsgemäßer Benutzerwechsel bei Video-Endpunkten
- Versehentliche bzw. unabsichtliche Preisgabe von Informationen
- Unzureichende Prüfung der Identität von Kommunikationspartnern
- Fehlverhalten und Missbrauch von Sprachsteuerung und KI-Funktionen
- Übergreifende Wirkung eines Sicherheitsvorfalls
- Konfigurationsfehler bei Videokonferenzlösungen
- Missbrauch von Administrations- und Wartungszugängen
- Unzureichende Organisation des Betriebs eines Videokonferenzsystems
- Unzureichendes Identitäts- und Berechtigungskonzept
- Unzureichend abgesicherte Aufzeichnung, Protokollierung und Dateiablage
- Unzureichende Kenntnis von Technik und Regelungen

Daraus ergeben sich die folgenden Sicherheitsanforderungen für Kollaborationswerkzeuge:

- Absicherung der zugrundeliegenden Technik und der Arbeitsumgebung (z.B. keine sensiblen Informationen im Blickfeld der Kamera, Ausblenden des Hintergrunds, keine Videokonferenzen in Großraumbüros)
- Sicherer Umgang mit Daten der Beitragenden (z.B. Teilnehmer von Videokonferenzen)

- Aufsetzen einer sicheren Benutzerverwaltung und Erstellen unterschiedlicher Nutzungsprofile
- Verschlüsseltes Speichern der Metadaten
- Absicherung von Dateiablagen und frei zugänglichen Endpunkten
- Gesichertes Aufbauen sowie Beenden von Sitzungen (sog. Sessions)
- Verwenden einer gesicherten Netzwerkverbindung
- Sicheres Beschaffen der Kollaborationswerkzeuge
- Erstellen und Bereitstellen von Informationen zur sicheren Verwendung von Kollaborationswerkzeugen
- Integrieren in bestehendes Update- bzw. Patchmanagement sowie Backup-Verfahren
- Deaktivieren nicht notwendiger Dienste bzw. Services (z.B. Sprachsteuerung, lokaler Zugriff auf Daten, automatische Rufannahme, Kamera-Zugriff) oder geeignetes Absichern
- Sicherstellen der Verfügbarkeit der Lösung (z.B. im eigenen Rechenzentrum, in einer Cloud)
- Aufsetzen eines Sicherheits- und Betriebskonzepts für Kollaborationswerkzeuge
- Vermeiden von Aufzeichnungen und Deaktivieren der Sprachsteuerung
- Darauf achten, dass etwaige aufgezeichnete bzw. protokollierte Daten, wo notwendig, in der EU gespeichert und abgelegt werden

[Quelle: BSI KoViKo]

6.3.6 Regelung des Dokumenten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

Damit der Austausch von Dokumenten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution sicher vollzogen werden kann, ist eine Regelung über die Art und Weise des Austausches aufzustellen.

Darin sollten zumindest folgende Punkte betrachtet bzw. geregelt werden:

- welche Dokumente bzw. Datenträger über welchen Transportweg (Postweg, Kurier, Paketdienst, …) ausgetauscht werden dürfen,
- welche Schutzmaßnahmen beim Transport zu beachten sind (beispielsweise Transport in geschlossenem Behälter, in Versandtasche, per Einschreiben, mit Begleitschreiben oder mit Versiegelung) und
- welche Dokumente bzw. Datenträger nur persönlich transportiert werden dürfen.

Da Schriftstücke oftmals Unikate sind, muss bei der Auswahl eines geeigneten Dokumentenaustauschverfahrens beachtet werden, welchen Schaden der Verlust bedeuten würde. Hingegen kann beim Datenträgeraustausch vorab eine Datensicherung erfolgen.

6.3.7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

Dienstliche Unterlagen und Datenträger dürfen auch am häuslichen Arbeitsplatz nur autorisierten MitarbeiterInnen zugänglich sein. Aus diesem Grund muss ein verschließbarer Bereich (Rollcontainer, Schrank, Schreibtisch o.ä.) verfügbar sein.

Die dienstlichen Unterlagen und Datenträger müssen außerhalb der Nutzungszeit darin verschlossen aufbewahrt werden. Die Schutzwirkung des abschließbaren Bereiches hat den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger zu entsprechen.

Backup-Datenträger müssen im häuslichen Bereich verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur die TelearbeiterInnen selbst bzw. deren Vertretungen darauf Zugriff haben. Jeweils eine Generation der Backup-Datenträger sollte jedoch in der Institution aufbewahrt werden, damit im Katastrophenfall die VertreterInnen auf die Backup-Datenträger zugreifen können.

6.3.8 Betreuungs- und Wartungskonzept für Telearbeitsplätze

Für die Telearbeitsplätze muss ein spezielles Betreuungs- und Wartungskonzept erstellt werden.

Dieses sollte folgende Punkte vorsehen:

- Benennen von problembezogenen AnsprechpartnerInnen für den Benutzerservice:
  An diese Stelle wenden sich TelearbeiterInnen bei Software- und Hardwareproblemen. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfestellung zu leisten bzw. leitet Wartungs- und Reparaturarbeiten ein.
- Wartungstermine:
  Die Termine für vor Ort durchzuführende Wartungsarbeiten sollten frühzeitig bekannt gegeben werden, damit die TelearbeiterInnen zu diesen Zeiten den Zutritt zum häuslichen Arbeitsplatz gewährleisten können.
- Einführung von Standardtelearbeitsrechnern:

Wenn möglich sollten alle TelearbeiterInnen einer Institution einen definierten Standardtelearbeitsrechner haben. Dies verringert den konzeptionellen und administrativen Aufwand für den Aufbau eines sicheren Telearbeitsrechners und erleichtert Problemlösungen für den Benutzerservice.

- Fernwartung:
  Falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann (z.B. Einspielen von Sicherheitsaktualisierungen, Installation bzw. Entfernung notwendiger Programme), sind die notwendigen Sicherheitsmaßnahmen sowie die erforderlichen Online-Zeiten zu vereinbaren. Insbesondere ist ein Sicherungsverfahren festzulegen, um den Missbrauch eines Fernwartungszugangs zu verhindern (vgl. 14.6.3 Fernwartung).
- Transport der IT:
  Es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, IT-Komponenten zwischen Institution und häuslichen Arbeitsplätzen der TelearbeiterInnen zu transportieren.

6.3.9 Geregelte Nutzung der Kommunikationsmöglichkeiten

Für Telearbeit werden typischerweise verschiedene Möglichkeiten zur Kommunikation wie beispielsweise Telefon-, Internet- bzw. VPN-Anbindung, aber auch Postaustausch sowie Akten- und Datenträgertransport benötigt, diese müssen daher vom Telearbeitsrechner unterstützt werden. Es muss auch geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen; etwa ob private Nutzung erlaubt oder untersagt sein soll.

Die Regelungen über die Nutzung der Kommunikationsmöglichkeiten bei Telearbeit sind schriftlich zu fixieren, z. B. in der Sicherheitsrichtlinie zur Telearbeit (siehe 6.3.4 Regelungen für Telearbeit bzw. Homeoffice). Diese Regelungen sind den TelearbeiterInnen auszuhändigen.

Zu klären sind zumindest folgende Punkte:

- Datenflusskontrolle
  - Welche Dienste dürfen zur Datenübertragung genutzt werden?
  - Welche Dienste dürfen zu Kollaborationszwecken (z.B. Videokonferenzen, Bearbeitung von Daten für mehrere Beteiligte) verwendet werden?
  - Welche Dienste dürfen explizit nicht genutzt werden?
  - Welche Informationen dürfen an wen versendet werden?
  - Welcher Schriftverkehr darf über E-Mail, Messenger-Apps oder Cloud-Dienste abgewickelt werden?

    - Falls am Telearbeitsplatz ein Faxgerät vorhanden ist, so ist zu klären, welche Informationen per Fax an wen übermittelt werden dürfen.
    - Der elektronische Versand welcher Informationen bedarf der vorherigen Zustimmung der Institution?
- Informationsgewinnung
    - Welche elektronischen Dienstleistungen (Datenbankabfragen, elektronische Recherchen) dürfen vom Telearbeitsrechner aus in Anspruch genommen werden? Beispielsweise können aus der Art der Abfragen u.U. Rückschlüsse auf Unternehmensstrategien gezogen werden.
- IT-Sicherheitsmaßnahmen
    - Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden?
    - Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Dies kann beispielsweise für personenbezogene Daten gelten.
    - Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
    - Wird vor Versand oder nach Erhalt von Daten ein Viren-Check der Daten durchgeführt?
    - Für welche Datenübertragung soll eine Protokollierung erfolgen? Falls eine automatische Protokollierung nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.
- Internetnutzung
    - Wird die Nutzung von Internetdiensten generell verboten?
    - Welche Art von Daten darf aus dem Internet geladen werden? Werden Daten von fremden Servern geladen, so besteht die Gefahr, dass Viren importiert werden.
    - Welche Optionen dürfen im Internet-Browser aktiviert werden?
    - Welche Rahmenbedingungen und technischen Sicherheitsmaßnahmen müssen bei der Internetnutzung beachtet werden? Welche Sicherungsverfahren sollen im Internet-Browser aktiviert werden?
    - Ist die Zustimmung der Institution erforderlich, wenn die TelearbeiterInnen sich am Informationsaustausch mittels Sozialen Medien oder Foren beteiligen wollen? Ggf. ist eine anonyme Nutzung erforderlich.
- Unterschriftenregelung
    - Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
    - Werden gesetzeskonforme elektronische Signaturen eingesetzt?
    - Werden andere Authentisierungsverfahren für den Schriftverkehr genutzt?

6.3.10 Regelung der Zugriffsmöglichkeiten von TelearbeiterInnen

Erfordert die Telearbeit den Zugriff auf die IT der Institution (zum Beispiel auf einen Server), muss zuvor festgelegt werden, welche Objekte (Daten, Programme, IT-Komponenten) die TelearbeiterInnen tatsächlich für die Erfüllung ihrer Aufgaben benötigen. Entsprechend sind die notwendigen Rechte wie Lese- und Schreibrechte auf diese Objekte zuzuweisen.

Auf Objekte, die die TelearbeiterInnen für ihre Aufgaben nicht brauchen, sollten sie auch nicht zugreifen können. Dies gilt sowohl für den Zugriff auf Daten wie auf in der Institution verfügbare IT-Komponenten. Damit soll erreicht werden, dass der Schaden, der aufgrund eines Hacker-Angriffs auf den Kommunikationsrechner entstehen kann, minimiert wird.

6.3.11 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution

Erfolgt im Rahmen der Telearbeit eine Datenübertragung zwischen einem Telearbeitsrechner und einem Kommunikationsrechner der Institution, werden dabei dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Institution noch die TelearbeiterInnen großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind ggf. zusätzliche Maßnahmen erforderlich, falls das öffentliche Netz keine ausreichende Sicherheit bieten kann.

Generell muss die Datenübertragung zwischen Telearbeitsrechner und Institution folgende Sicherheitsanforderungen erfüllen:

- Sicherstellung der Vertraulichkeit der übertragenen Daten:
  Es muss durch eine ausreichend sichere Verschlüsselung erreicht werden, dass auch durch Abhören der Kommunikation zwischen Telearbeitsrechner und Kommunikationsrechner der Institution kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- Sicherstellung der Integrität der übertragenen Daten:
  Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben. Bei Bedarf kann auch ein zusätzlicher Fehlererkennungsmechanismus benutzt werden, um absichtliche Manipulationen während der Datenübertragung erkennen zu können (vgl. dazu § 126a Datenbeschädigung (StGB)).

- Sicherstellung der Verfügbarkeit der Datenübertragung:
  Falls zeitliche Verzögerungen bei der Telearbeit nur schwer zu tolerieren sind, sollte ein redundant ausgelegtes öffentliches Kommunikationsnetz als Übertragungsweg ausgewählt werden, in dem der Ausfall einzelner Verbindungsstrecken nicht den Totalausfall der Kommunikationsmöglichkeiten bedeutet. Auf eine redundante Einführung der Netzanbindung an den Telearbeitsrechner und die Schnittstelle der Institution kann ggf. verzichtet werden.
- Sicherstellung der Authentizität der Daten:
  Bei der Übertragung der Daten zwischen Telearbeitsrechner und Institution muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen TeilnehmerInnen stattfindet, so dass eine Maskerade ausgeschlossen werden kann. Dies bedeutet, dass Daten mit Absender „Telearbeitsrechner“ auch tatsächlich von dort stammen. Ebenso muss der Ursprung von Institutionsdaten zweifelsfrei auf die Institution zurückgeführt werden können.
- Sicherstellung der Nachvollziehbarkeit der Datenübertragung:
  Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.
- Sicherstellung des Datenempfangs:
  Ist es für die Telearbeit von Bedeutung, ob Daten korrekt empfangen wurden, so können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob die EmpfängerInnen die Daten korrekt empfangen haben.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten.

6.3.12 Sicherheitstechnische Anforderungen an den Kommunikationsrechner

Je nach Art der Telearbeit und der dabei durchzuführenden Aufgaben gestaltet sich der Zugriff der TelearbeiterInnen auf Institutionsdaten anders. So ist denkbar, dass zwischen TelearbeiterInnen und Institution nur E-Mails ausgetauscht werden. Andererseits kann auch ein Zugriff auf Server oder Cloud-Dienste in der Institution notwendig sein.

Unabhängig von den Zugriffsweisen muss der Kommunikationsrechner der Institution i. Allg. folgende Sicherheitsanforderungen erfüllen:

- Identifikation und Authentisierung:
  Sämtliche BenutzerInnen des Kommunikationsrechners, also AdministratorInnen, MitarbeiterInnen in der Institution und TelearbeiterInnen, müssen sich vor einem Zugriff auf den Rechner identifizieren und authentisieren. Nach mehrfachen Fehlversuchen ist der Zugang zu sperren. Voreingestellte

Passwörter sind zu ändern. Ggf. muss es für den Kommunikationsrechner auch möglich sein, während der Datenübertragung eine erneute Authentisierung der TelearbeiterInnen oder der Telearbeitsrechner anzustoßen, um aufgeschaltete AngreiferInnen abzuwehren. Im Rahmen der Identifikation und Authentisierung der BenutzerInnen sollte auch zusätzlich eine Identifizierung der Telearbeitsrechner stattfinden.

- Rollentrennung:
  Die Rollen der AdministratorInnen und der BenutzerInnen des Kommunikationsrechners sind zu trennen. Eine Rechtevergabe darf ausschließlich AdministratorInnen möglich sein.
- Rechteverwaltung und -kontrolle:
  Der Zugriff auf Dateien des Kommunikationsrechners darf nur im Rahmen der gebilligten Rechte erfolgen können. Der Zugriff auf angeschlossene Rechner in der Institution und darauf gespeicherte Dateien ist zu reglementieren. Dabei ist darauf zu achten, dass die Zugriffsmöglichkeiten auf das notwendige Mindestmaß beschränkt werden. Bei Systemabsturz oder bei Unregelmäßigkeiten muss der Kommunikationsrechner in einen sicheren Zustand übergehen, in dem ggf. kein Zugriff mehr möglich ist.
- Minimalität der Dienste:
  Dienste, die durch den Kommunikationsrechner zur Verfügung gestellt werden, müssen dem Minimalitätsprinzip unterliegen: alles ist verboten, was nicht ausdrücklich erlaubt wird. Die Dienste selbst sind auf den Umfang zu beschränken, der für die Aufgaben der TelearbeiterInnen notwendig ist.
- Protokollierung:
  Datenübertragungen vom, zum und über den Kommunikationsrechner sind mit Uhrzeit, BenutzerIn, Adresse und Dienst zu protokollieren. Den AdministratorInnen bzw. der Revision sollten Werkzeuge zur Verfügung stehen, um die Protokolldaten auszuwerten. Dabei sollten Auffälligkeiten automatisch gemeldet werden.
- Automatische Virenprüfung:
  Übertragene Daten sind einer automatischen Prüfung auf Viren zu unterziehen.
- Verschlüsselung:
  Daten, die auf dem Kommunikationsrechner für die TelearbeiterInnen vorgehalten werden, sind bei entsprechender Vertraulichkeit - in Abstimmung mit der organisationsweiten IT-Sicherheitspolitik - zu verschlüsseln.
- Vermeidung oder geeignete Absicherung von Fernadministration:
  Benötigt der Kommunikationsrechner keine Fernadministration, so sind sämtliche Funktionalitäten zur Fernadministration zu sperren. Ist eine Fernadministration unvermeidbar (z.B. für die Einspielung von Sicherheitsaktualisierungen oder zur Installation bzw. Entfernung notwendiger Programme), so muss sie ausreichend abgesichert werden. Jegliche

Fernadministration darf nur nach vorhergehender erfolgreicher Identifikation und Authentisierung stattfinden. Administrationstätigkeiten sind zu protokollieren. Administrationsdaten sollten verschlüsselt übertragen werden. Voreingestellte Passwörter und kryptographische Schlüssel sind zu ändern.

6.3.13 Informationsfluss, Meldewege und Fortbildung

Damit die TelearbeiterInnen nicht vom betrieblichen Geschehen abgeschnitten werden, sollte die Vorgesetzten einen regelmäßigen Informationsaustausch zwischen TelearbeiterInnen und den ArbeitskollegInnen ermöglichen. Dies ist wichtig, damit die TelearbeiterInnen auch zukünftig über Planungen und Zielsetzungen in ihrem Arbeitsbereich informiert sind, damit Frustrationen vermieden werden und ein positives Telearbeitsklima geschaffen wird und erhalten bleibt.

Die Beteiligung der TelearbeiterInnen an Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften ist zu regeln. Dies stellt dann ein Problem dar, wenn die TelearbeiterInnen ausschließlich zu Hause arbeiten. Eine Lösung wäre eventuell das Einscannen wichtiger Schriftstücke, um sie dann den TelearbeiterInnen per E-Mail zuzustellen. Zusätzlich sind die TelearbeiterInnen insbesondere über Änderungen von IT-Sicherheitsmaßnahmen zu unterrichten.

Weiters müssen die ArbeitskollegInnen über Anwesenheits- und Erreichbarkeitszeiten sowie die E-Mail-Adressen bzw. Telefonnummern der TelearbeiterInnen in Kenntnis gesetzt werden (z.B. über eine Kontaktliste oder Einträge im Intranet).

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechperson bei technischen oder organisatorischen Problemen in der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese von den TelearbeiterInnen unverzüglich der Institution gemeldet werden.

Da für die Telearbeit zum Teil andere IT-Sicherheitsmaßnahmen ergriffen werden müssen als für die Arbeit innerhalb der Institution, ist es notwendig, dass ein Sicherheitskonzept für die Telearbeitsplätze erstellt wird. Nach Bekanntgabe des Konzeptes müssen TelearbeiterInnen in die zu realisierenden

Sicherheitsmaßnahmen eingewiesen und eventuell in ihrem Umgang geschult werden. Darüber hinaus sind die TelearbeiterInnen so weit im Umgang mit den Telearbeitsrechnern zu schulen, dass sie einfache Tätigkeiten wahrnehmen bzw. einfache Probleme selbstständig lösen können.

6.3.14 Vertretungsregelung für Telearbeit

Über die Maßnahme 7.1.3 Vertretungsregelungen hinaus sind im Falle der Vertretung von TelearbeiterInnen weitere Schritte notwendig. Da die TelearbeiterInnen hauptsächlich außerhalb der Institution tätig sind, muss ein Informationsfluss zu ihrer Vertretung vorgesehen werden. Auch eine Dokumentation der Arbeitsergebnisse seitens der TelearbeiterInnen ist unabdingbar. Ggf. sind sporadische oder regelmäßige Treffen zwischen TelearbeiterInnen und ihren Vertretungen sinnvoll.

Ergänzend dazu muss geregelt werden, wie VertreterInnen im unerwarteten Vertretungsfall Zugriff auf die Daten welche auf dem Telearbeitsrechner gespeichert sind oder am Telearbeitsplatz vorhandene Unterlagen nehmen können. Auch der Zugriff auf erstellte – verschlüsselte – Backups kann davon umfasst sein.

Es empfiehlt sich, den Vertretungsfall probeweise durchzuspielen.

6.3.15 Entsorgung von Datenträgern und Dokumenten

Auch zu Hause oder unterwegs gibt es häufiger Material, das entsorgt werden soll, schon alleine deshalb, damit das Gepäck noch tragbar bleibt. Während es aber innerhalb der eigenen Institution eingeübte Verfahren gibt, wie alte oder unbrauchbare Datenträger und Dokumente entsorgt werden, ist dies am häuslichen Arbeitsplatz oder unterwegs nicht immer möglich.

Im Lebenszyklus von Daten bzw. Informationen spielt auch deren sichere Entsorgung eine große Rolle. Eine Sicherheitsrichtlinie sollte demzufolge regeln, wie insbesondere schutzbedürftige Daten bzw. Arbeitsmaterialien zu beseitigen bzw. entsorgen sind, um die relevanten Gefahren zu adressieren.

Gefahren zur Entsorgung von Datenträgern und Daten sind:

- Fehlende oder unzureichend dokumentierte Regelungen beim Löschen und Vernichten
- Vertraulichkeitsverlust durch Restinformationen auf Datenträgern
- Ungeeignete Einbindung externer Dienstleister in das Löschen und Vernichten

Vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen bzw. zu prüfen, ob diese sensible Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder in geschützter Form an den Standort der Organisation bzw. Institution zurücktransportiert werden, um dort in geeigneter Weise entsorgt zu werden. Dies ist auch dann erforderlich, wenn die Datenträger defekt sind, da ExpertInnen auch hieraus wieder wertvolle Informationen zurückgewinnen können. Auch Shredder-Einrichtungen in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist. Der Hausmüll, der nächste Papierkorb im Hotel bzw. der Bahn oder vergleichbare Einrichtungen sind jedenfalls nicht dafür geeignet, solche Datenträger zu entsorgen.

Daraus ergeben sich die folgenden Anforderungen zur sicheren Entsorgung von Datenträgern und Daten:

- Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen
- Löschung und Vernichtung von Datenträgern durch externe Dienstleister
- Mindestanforderungen an Verfahren zur Löschung und Vernichtung
- Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern
- Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen
- Vernichtung defekter digitaler Datenträger
- Vernichten von Datenträgern auf erhöhter Sicherheitsstufe

[Quelle: BSI CON.6, INF.8, INF.9]

7 Personelle Sicherheit

Die MitarbeiterInnen stellen eine der wichtigsten Ressourcen einer Organisation dar. IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die MitarbeiterInnen ein ausgeprägtes Sicherheitsbewusstsein haben und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen MitarbeiterInnen auch potenzielle Angriffs- oder Fehlerquellen dar.

Aus diesen Gründen sind der Schulung und Sensibilisierung für Fragen der IT-Sicherheit eine besondere Bedeutung zuzumessen. Darüber hinaus ist es auch notwendig, sich mit den Möglichkeiten und potenziellen Problemen von MitarbeiterInnen auseinander zu setzen („Know your Employee“).

Im Folgenden werden in 7.1 Regelungen für MitarbeiterInnen Regelungen angeführt, die teilweise sinngemäß auch für Fremdpersonal gelten, 7.2 Regelungen für den Einsatz von Fremdpersonal gibt einige spezielle Regelungen für Fremdpersonal.

7.3 Sicherheitssensibilisierung und -schulung schließlich führt Maßnahmen zur Sensibilisierung und Schulung im Bereich IT-Sicherheit auf.

7.1 Regelungen für MitarbeiterInnen

7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Bei der Einstellung von MitarbeiterInnen sind diese zur Einhaltung einschlägiger Gesetze (z. B. Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz) § 6 „Datengeheimnis“, Datenschutz-Grundverordnung (DSGVO) Artikel 32 „Sicherheit der Verarbeitung“ und Artikel 44 „Allgemeine Grundsätze der Datenübermittlung“ ff. (im sicherheitspolizeilichen Bereich auch DSG § 54 „Datensicherheitsmaßnahmen“ und DSG § 58 „Allgemeine Grundsätze für die Übermittlung personenbezogener Daten“), sowie dem Informationssicherheitsgesetz für den Bereich der öffentlichen Verwaltung), Vorschriften und interner Regelungen zu verpflichten.

Damit sollen neue MitarbeiterInnen mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die MitarbeiterInnen an zentraler Stelle zur Einsichtnahme vorzuhalten.

Neben der Verpflichtung zur Einhaltung von Gesetzen und Vorschriften empfiehlt es sich insbesondere, Regelungen zu folgenden Bereichen zu treffen, die dann auch in eine entsprechende Verpflichtungserklärung aufzunehmen sind:

- Clear-Desk-Policy, falls vorgesehen (vgl. 7.1.7 Clear-Desk-Policy)
- Einhaltung von PC-Benutzungsregeln (vgl. 8.1.3.1 Herausgabe einer PC-Richtlinie)
- Einhaltung der Regeln für die Benutzung des Internet (siehe 13.1.10 Remote Access (VPN) - Konzeption und C.1 Wichtige Normen).

7.1.2 Aufnahme der sicherheitsrelevanten Aufgaben und Verantwortlichkeiten in die Stellenbeschreibung

Bei der Erstellung von Stellenbeschreibungen ist dafür Sorge zu tragen, dass alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit in diese Beschreibungen aufgenommen werden. Anzuführen sind dabei sowohl die allgemein aus der organisationsweiten IT-Sicherheitspolitik abzuleitenden Verpflichtungen als auch spezielle Verantwortlichkeiten auf Grund der Tätigkeit.

Dies gilt in besonderem Maße für MitarbeiterInnen mit speziellen Sicherheitsaufgaben (Mitglieder des IT-Sicherheitsmanagement-Teams, Datenschutzbeauftragte, CISO, Informationssicherheitskoordinatoren im Bereich, Applikations-/Projektverantwortliche).

7.1.3 Vertretungsregelungen

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen sowie eine zeitgerechte Einarbeitung unkundiger MitarbeiterInnen unbedingt erforderlich sind.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Die VertreterInnen müssen so geschult werden, dass sie die Aufgaben jederzeit übernehmen können. Stellt sich heraus, dass es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, VertreterInnen zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Die VertreterInnen dürfen die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen kompetente VertreterInnen zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.
- Es sollte vermieden werden, dass Vertretungsregeln u.U. vorgesehene Mehraugenprinzipien unterlaufen, z. B. wenn sich zwei kollektiv Berechtigte wechselseitig vertreten.
- Im Zusammenhang mit der Verwendung von kryptographischen Systemen ist auch über ein Verfahren zur Offenlegung von kryptographischen Schlüsseln im Rahmen des Kryptokonzeptes zu achten (siehe auch 10.1 Kryptographische Maßnahmen).

7.1.4 Geregelte Verfahrensweise beim Ausscheiden von MitarbeiterInnen

Scheiden MitarbeiterInnen aus, so sollten einige Punkte beachtet werden.

Dies wären:

- Vor dem Ausscheiden ist eine Einweisung der NachfolgerInnen durchzuführen.
- Von den Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z. B. Laptops, Smartphones, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen.
- Es sind sämtliche für die Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

- Es ist sicherzustellen, dass bei Ausscheidenden keine Unterlagen, Betriebsmittel oder Zugangsmöglichkeiten verbleiden, und diese Nachfolgenden für ihre Tätigkeiten zur Verfügung stehen.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeit erhaltenen Informationen weitergegeben werden dürfen.
- Nach Möglichkeit sollte eine Neuvergabe der User-IDs an andere MitarbeiterInnen vermieden/ausgeschlossen werden.
- Sind die ausscheidenden Personen FunktionsträgerInnen in einem Notlaufplan, so ist der Notlaufplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Portierdienst, sind über das Ausscheiden der MitarbeiterInnen zu unterrichten.
- Ausgeschiedenen MitarbeiterInnen ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren.
- Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.
- Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten der Ausscheidenden vorgezeichnet sind, die sie vor Verlassen der Behörde bzw. des Unternehmens zu erledigen haben.

7.1.5 Geregelte Verfahrensweise bei Versetzung von MitarbeiterInnen

Bei Versetzung von MitarbeiterInnen oder einer wesentlichen Änderung ihrer Tätigkeit sind ihre Zugangsberechtigungen sowie Zugriffsrechte auf Übereinstimmung mit den neuen Anforderungen zu überprüfen und gegebenenfalls anzupassen.

7.1.6 Gewährleistung eines positiven Betriebsklimas

Ein positives Betriebsklima motiviert die MitarbeiterInnen einerseits zur Einhaltung von IT-Sicherheitsmaßnahmen und bewirkt andererseits die Reduzierung von fahrlässigen oder vorsätzlichen Handlungen (vgl. § 126a Datenbeschädigung (StGB)), die eine Störung des IT-Betriebs herbeiführen können. Daher sollte auch unter IT-Sicherheitsaspekten versucht werden, ein positives Betriebsklima zu erreichen.

Dazu gehört auch die ergonomische Gestaltung des Arbeitsplatzes. Hierzu besteht eine Reihe von Regelungen und Normen, deren Nichtbeachtung u. a. eventuell zu Sicherheitsproblemen führen kann. Ergonomie ist nicht Gegenstand dieses Handbuches, die Wichtigkeit einer ergonomischen Gestaltung des Arbeitsplatzes sei aber hier nochmals betont.

Weiters ist bei der Ausstattung von Arbeitsplätzen darauf zu achten, dass die Einhaltung von IT-Sicherheitsmaßnahmen unterstützt wird. Dazu gehören etwa verschließbare Schreibtische oder Schränke, in denen Datenträger, Dokumentationen, Unterlagen und Zubehör verschlossen werden können.

Ursache für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme von ArbeitnehmerInnen sein. Daher ist es für jede Organisation wichtig, ihre MitarbeiterInnen und eventuelle potenzielle Probleme zu kennen („Know your Employee“). In vielen Fällen kann es hilfreich sein, wenn eine Anlaufstelle zur Verfügung steht, die bei solchen Problemen konkrete Hilfe und Lösungsmöglichkeiten anbieten kann.

7.1.7 Clear-Desk-Policy

Alle MitarbeiterInnen sollten vor ihrer Abwesenheit ihre Unterlagen und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank, PC und Telefon. Dies gilt insbesondere für Großraumbüros, aber auch in den anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (BesucherInnen, Reinigungspersonal, unbefugte MitarbeiterInnen, …) Zugriff zu Schriftstücken, Datenträgern und IT-Komponenten haben.

Ist eine „Clear-Desk-Policy“-Regelung in einer Organisation vorgesehen, so sollte die Einhaltung dieser Regelung in die Verpflichtungserklärung aller MitarbeiterInnen (vgl. 7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen) aufgenommen werden.

7.1.8 Benennung vertrauenswürdiger AdministratorInnen und VertreterInnen

AdministratorInnen von IT-Systemen und ihren VertreterInnen müssen vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals allumfassende Befugnisse. AdministratorInnen und ihre VertreterInnen sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre.

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden. Es soll regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen. Eine regelmäßige Kontrolle von AdministratorInnen - etwa durch Auswertung von Protokollen durch Revisoren - ist vorzusehen.

Darüber hinaus sollte geprüft werden, inwieweit durch technische Maßnahmen - etwa die Verschlüsselung von ausgewählten Daten oder Zugriffsbeschränkungen zu Protokollfiles - die Befugnisse von AdministratorInnen eingeschränkt werden können, ohne deren Aufgabenerfüllung zu beeinträchtigen.

7.1.9 Verpflichtung der PC-BenutzerInnen zum Abmelden

Wird ein PC von mehreren BenutzerInnen genutzt und besitzen die einzelnen BenutzerInnen unterschiedliche Zugriffsrechte auf im PC gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn alle BenutzerInnen sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmelden. Ist es Dritten möglich, an einem PC unter der Identität von Anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle PC-BenutzerInnen zu verpflichten, sich bei Verlassen des Arbeitsplatzes abzumelden.

Ist keine Zugriffskontrolle realisiert, so ist die Abmeldung der BenutzerInnen aus Gesichtspunkten der Ordnungsmäßigkeit dennoch vorzuschreiben.

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch eine manuelle oder nach einer gewissen Zeit automatische Aktivierung der Bildschirmsperre erfolgen.

7.1.10 Kontrolle der Einhaltung der organisatorischen Vorgaben

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die BenutzerInnen eines IT-Systems die organisatorischen Vorgaben (etwa Verpflichtung zur Abmeldung nach Aufgabenerfüllung oder Verbot der Weitergabe von Passwörtern) auch tatsächlich einhalten.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz von Kontrollen ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass dabei keine Personen bloßgestellt werden oder als „Schuldige“ identifiziert werden. Wenn die MitarbeiterInnen dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Wenn MitarbeiterInnen eine Regelung ignorieren oder umgehen, ist das meist ein Zeichen dafür, dass diese nicht mit den Arbeitsabläufen vereinbar ist oder durch die MitarbeiterInnen nicht umgesetzt werden kann. Beispielsweise ist eine Anweisung, vertrauliche Schreiben nicht unbeaufsichtigt am Drucker liegen zu lassen, unsinnig, wenn zum Drucken nur ein weit entfernter Netzdrucker zur Verfügung steht.

Wenn bei Kontrollen Mängel festgestellt werden, kommt es nicht darauf an, nur die Symptome zu beseitigen. Vielmehr ist es wichtig, die Ursachen für diese Probleme festzustellen und Lösungen aufzuzeigen. Diese können beispielsweise in der Änderung bestehender Regelungen oder in der Hinzunahme technischer Maßnahmen bestehen.

7.1.11 Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen

Die Vorgehensweise zur Untersuchung angeblicher (bewusster oder versehentlicher) Verletzungen von Sicherheitsvorgaben sowie potenzielle Konsequenzen - im Falle interner MitarbeiterInnen können dies beispielsweise disziplinäre Maßnahmen sein, im Falle externer MitarbeiterInnen etwa vertraglich abgeleitete Konsequenzen - sollen festgelegt, vom Management verabschiedet und allen MitarbeiterInnen bekannt sein.

Eine derartig geregelte Verfahrensweise kann einerseits infolge der abschreckenden Wirkung zur Prävention von Sicherheitsverletzungen dienen und gewährleistet andererseits eine korrekte und faire Behandlung von Personen, denen Sicherheitsverletzungen angelastet werden.

7.2 Regelungen für den Einsatz von Fremdpersonal

7.2.1 Regelungen für den kurzfristigen Einsatz von Fremdpersonal

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie BesucherInnen zu behandeln, d. h. dass also etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von MitarbeiterInnen der Behörde bzw. des Unternehmens erlaubt ist etc. (vgl. dazu etwa 11.1.6 Portierdienst).

7.2.2 Verpflichtung externer MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Externe MitarbeiterInnen, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und evtl. Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind ebenfalls schriftlich zur Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

In B Muster für Verträge, Verpflichtungserklärungen und Dokumentationen werden Beispiele für die Formulierung derartiger Verpflichtungserklärungen gegeben.

7.2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

Fremde (BesucherInnen, HandwerkerInnen, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch 11.1.4 Zutrittskontrolle und 11.1.6 Portierdienst). Wird es erforderlich, Fremde allein im Büro zurückzulassen, sollte man KollegInnen ins Zimmer oder die BesucherInnen zu KollegInnen bitten.

Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Schloss für Laufwerk, Tastaturschloss), sowie mobile Geräte mit einem Kensington-Schloss oder Ähnlichem gesichert werden. Siehe auch 7.1.7 Clear-Desk-Policy.

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und BesucherInnen sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugangsschutz gesichert ist (vgl. 6.3.3 Geeignete Einrichtung eines häuslichen Arbeitsplatzes und 6.3.4 Regelungen für Telearbeit bzw. Homeoffice).

Die Notwendigkeit dieser Maßnahmen ist den MitarbeiterInnen zu erläutern und ggf. in einer Dienstanweisung festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

7.2.4 Information externer MitarbeiterInnen über die IT-Sicherheitspolitik

Externe MitarbeiterInnen sind - soweit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten.

7.3 Sicherheitssensibilisierung und -schulung

7.3.1 Geregelte Einarbeitung/Einweisung neuer MitarbeiterInnen

Neuen MitarbeiterInnen müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre AnsprechpartnerInnen bzgl. IT-Sicherheit nicht. Sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik die Behörde bzw. das Unternehmen betreibt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen. Daher kommt der geregelten Einarbeitung neuer MitarbeiterInnen eine entsprechend hohe Bedeutung zu.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Planung der notwendigen Schulungen; arbeitsplatzbezogene Schulungsmaßnahmen (siehe auch 7.3.2 Schulung vor Programmnutzung und 7.3.3 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen),
- Vorstellung aller AnsprechpartnerInnen, insbesondere zu IT-Sicherheitsfragen,
- Erläuterung der hausinternen Regelungen und Vorschriften zur IT-Sicherheit und der organisationsweiten IT-Sicherheitspolitik.

7.3.2 Schulung vor Programmnutzung

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die BenutzerInnen eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die BenutzerInnen vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden.

Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen. Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

Stehen leicht verständliche Handbücher oder Anleitungen zu IT-Anwendungen bereit, so kann an Stelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

7.3.3 Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen

Umfassende IT-Sicherheit kann nur dann gewährleistet werden, wenn alle beteiligten und betroffenen Personen einen angemessenen Kenntnisstand über IT-Sicherheit allgemein und insbesondere über die Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet haben. Es liegt in der Verantwortung der Organisationsleitung, durch geeignete Schulungsmaßnahmen hierfür die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte alle BenutzerInnen dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Angesichts des Umfangs der möglichen Schulungsthemen und der Bedeutung der IT-Sicherheit ist bei der Auswahl der Schulungsinhalte ein koordiniertes Vorgehen erforderlich. Dieses ist in Schulungskonzepten darzulegen und zu dokumentieren.

Es sollte versucht werden, Schulungsthemen zur IT-Sicherheit soweit möglich in andere Schulungskonzepte der betreffenden Organisation, etwa in die IT-Anwenderschulung, zu integrieren. Eine solche Einbindung hat den Vorteil, dass IT-Sicherheit unmittelbar als Bestandteil des IT-Einsatzes wahrgenommen wird.

Insbesondere sollen folgende Themen in der Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden:

- Sensibilisierung für IT-Sicherheit
  Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist jede/r Einzelne zum sorgfältigen Umgang mit der IT zu motivieren. Zusätzlich sind Verhaltensregeln zu vermitteln, die Verständnis für die IT-Sicherheitsmaßnahmen wecken. Alle MitarbeiterInnen sind auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze von dem reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, evtl. auch durch praktische Hinweise z. B. in hausinternen Publikationen, im Intranet oder am „Schwarzen Brett“.
- Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen MitarbeiterInnen umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.
- Die produktbezogenen IT-Sicherheitsmaßnahmen
  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Softwareprodukt verbunden sind und bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung, der Pausenschaltung durch Bildschirmschoner auch Möglichkeiten der Verschlüsselung von Dokumenten oder Datenfeldern sein. Hinweise und

Empfehlungen über die Strukturierung und Organisation von Dateien, die anwendungsspezifische Daten enthalten, können die Vergabe von Zugriffsrechten erleichtern und den Aufwand für die Datensicherung deutlich reduzieren.

- Das Verhalten bei Auftreten eines Schadprogramms
  Hier soll den MitarbeiterInnen vermittelt werden, wie mit Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe 12.3 Schutz vor Schadprogrammen und Schadfunktionen):
  - Wirkungsweise und Arten von Schadprogrammen
  - Vorbeugende Maßnahmen
  - Erkennen des Schadprogrammbefalls
  - Sofortmaßnahmen im Verdachtsfall
  - Maßnahmen zur Eliminierung des Schadprogrammes
- Der richtige Einsatz von Zugangscodes und weiteren Authentifizierungsmitteln
  Hierbei sollen die Bedeutung von Zugangscodes (Passwörtern, PINs etc.) und physischen Zugangskomponenten (Karten, Token, Smartphone, …) für die IT-Sicherheit erläutert werden. Ebenso sind die Randbedingungen, die einen wirksamen Einsatz von Zugangsfaktoren erst ermöglichen, herauszuarbeiten (vgl. auch 9.3.1 Regelungen des Passwortgebrauches und 9.6.2 Regelungen des Gebrauchs von Chipkarten).
- Die Bedeutung der Datensicherung und deren Durchführung
  Die regelmäßige Datensicherung ist eine der wichtigsten IT-Sicherheitsmaßnahmen in jedem IT-System. Vermittelt werden sollen das Datensicherungskonzept (siehe 12.4 Datensicherung) der Organisation und die von jeder/jedem Einzelnen durchzuführenden Datensicherungsaufgaben. Besonders bedeutend ist dies für persönliche Geräte (PC, Laptop, Smartphone), sofern die Benutzer/innen selbst die Datensicherung durchführen müssen.
- Der geregelte Ablauf eines Datenträgeraustausches
  Die Festlegung, wann welchen Kommunikationspartnern und -partnerinnen welche Datenträger übermittelt werden dürfen, ist allen Beteiligten bekannt zu geben. Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung, digitale Signaturen oder Checksummenverfahren), so sind die MitarbeiterInnen in die Handhabung dieser Verfahren ausreichend einzuarbeiten.
- Der Umgang mit personenbezogenen Daten
  An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter/innen, die mit personenbezogenen Daten (sowohl in IT-Systemen als auch in Akten bzw. Dokumenten) arbeiten müssen, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen, die sich insbesondere aus der Datenschutzgrundverordnung (DSGVO) bzw.

dem Datenschutzgesetz (DSG) ergeben, zu schulen. Dies betrifft etwa Meldepflichten, den Umgang mit den Rechten von Betroffenen (Auskunft, Berichtigung, Löschung, Verarbeitungseinschränkung, Datenübertragbarkeit, …), Datensicherheitsmaßnahmen sowie Übermittlung von Daten.

- Die Einweisung in Notfallmaßnahmen
  Sämtliche MitarbeiterInnen (auch nicht unmittelbar mit IT befasste Personen wie Portier oder Wachpersonal) sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehören die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer, der Umgang mit Feuerlöschern, das Notfallmeldesystem (wer als Erstes wie zu benachrichtigen ist) und der Umgang mit dem Disaster Recovery-Handbuch.
- Richtiges Verhalten bei Auftreten von Sicherheitsproblemen (IHP)
  Die in den Incident Handling-Plänen (IHPs) festgelegten Aufgaben und Verantwortlichkeiten aller MitarbeiterInnen bei Auftreten sicherheitsrelevanter Ereignisse sind allen betroffenen MitarbeiterInnen bekannt zu machen, regelmäßige Schulungen und gegebenenfalls praktische Übungen sind vorzusehen (vgl. auch 7.3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling-Pläne))
- Vorbeugung gegen „Social Engineering“
  Die MitarbeiterInnen sollen auf die Gefahren des „Social Engineerings“ hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden.
  Da „Social Engineering“ oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten MitarbeiterInnen regelmäßig darauf hingewiesen werden, die Identität von GesprächspartnerInnen zu überprüfen und insbesondere am Telefon und per E-Mail keine vertraulichen Informationen weiterzugeben.

7.3.4 Betreuung und Beratung von IT-BenutzerInnen

Neben der Schulung, die die IT-BenutzerInnen in die Lage versetzt, die vorhandene Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-BenutzerInnen für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardwaredefekten, fehlerhaften Softwareinstallationen, aber auch aus Bedienungsfehlern resultieren.

In größeren Behörden bzw. Unternehmen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der IT-BenutzerInnen zu beauftragen und diese allen MitarbeiterInnen bekannt zu geben („Helpdesk“). Dabei hat sich die Wahl einer besonders leicht zu merkenden Telefonnummer bzw. E-Mail-Adresse besonders bewährt. Die Einrichtung eines Helpdesk kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als vorteilhaft erweisen.

Es muss für alle BenutzerInnen klar ersichtlich sein, an wen sie sich in Problemfällen zu wenden haben.

7.3.5 Aktionen bei Auftreten von Sicherheitsproblemen (Incident Handling-Pläne)

Die Aufgaben und Verantwortlichkeiten aller MitarbeiterInnen bei Auftreten von sicherheitsrelevanten Ereignissen sollten im Rahmen der organisationsweiten IT-Sicherheitspolitik (High-Level-Beschreibung) sowie spezieller „Incident Handling-Pläne“ (IHPs) sowohl für einzelne Bereiche als auch für die gesamte Organisation festgelegt werden (vgl. dazu auch 16.1.3 Erstellung eines Incident Handling-Plans und Richtlinien zur Behandlung von Sicherheitsvorfällen).

Unter sicherheitsrelevanten Ereignissen sind dabei zu verstehen:

- Angriffe und (vermutete) Angriffsversuche gegen ein IT-System
- (vermutete) Sicherheitsschwächen
- Funktionsstörungen von Systemen (etwa durch schädliche Software)

Incident Handling-Pläne sollen in schriftlicher Form und verbindlich festlegen:

- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- die Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevanter Vorfälle,
- die einzuhaltenden Meldewege,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw. Gegenmaßnahmen treffen müssen.

IHPs sind allen betroffenen MitarbeiterInnen bekannt zu machen.

7.3.6 Schulung des Wartungs- und Administrationspersonals

Das Wartungs- und Administrationspersonal sollte mindestens so weit geschult werden, dass

- alltägliche Administrationsarbeiten selbst durchgeführt,
- einfache Fehler selbst erkannt und behoben,
- Datensicherungen selbsttätig durchgeführt,
- Tätigkeiten im Normalbetrieb bis zur Erkennung von Problemen eigenhändig durchgeführt,
- die Eingriffe von externem Wartungspersonal nachvollzogen und
- Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt

werden können.

7.3.7 Einweisung in die Regelungen der Handhabung von Kommunikationsmedien

Der Einsatz von Kommunikationsmedien und -Geräten - dazu zählen Soziale Medien und Messenger-Dienste, aber auch Smartphone, Router, Fax und Anrufbeantworter - erleichtert die Kommunikation, bringt aber auch neue potenzielle Gefährdungen der Vertraulichkeit und Integrität von Informationen mit sich. Alle MitarbeiterInnen sind daher auf die Besonderheiten der Handhabung von solchen Diensten und Geräten hinzuweisen und für potenzielle Gefahren zu sensibilisieren. Eine ausführliche Behandlung des Themas „Soziale Medien", inklusive Maßnahmen für deren Verwendung, ist im Anhang A.5 Sicherheit in sozialen Netzen zu finden. Grundsätzliche Anforderungen und Regelungen für die elektronische Kommunikation sind in 13.2 Informations- und Datenaustausch angeführt.

Verständliche Bedienungsanleitungen, Sicherheitshinweise und ggf. auch Dienstanweisungen sind den MitarbeiterInnen zur Kenntnis zu bringen und verfügbar zu halten.

Im Folgenden werden einige Beispiele angeführt, was solche Regelungen generell umfassen könnten. Sie sind den jeweiligen technischen Anforderungen und Möglichkeiten anzupassen.

Kommunikationsmedien

- Festlegung von Richtlinien für die Verwendung von Kommunikationsmedien (Wer darf welche Medien verwenden? Welche Art von Informationen dürfen wie versendet werden?),
- Verbot des Versendens von vertraulichen Informationen über bestimmte Kommunikationskanäle oder technische und organisatorische Vorkehrungen für das Versenden, je nach Vertraulichkeitsgrad (z.B. telefonische Vorankündigung, Verschlüsselung),
- ggf. Kontrolle der Einhaltung von Richtlinien.

Kommunikationsgeräte

- Information über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb der jeweiligen Geräte,
- Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Gerätes,
- Regelung über den Einsatz von Authentifizierungscodes zur Absicherung der Geräte oder der Kommunikation,
- Vermeidung schutzbedürftiger Informationen,
- Regelmäßige Säuberung aufgezeichneter oder gespeicherter Daten,
- Abschalten nicht benötigter Dienste und Komponenten.

7.3.8 Einweisung in die Bedienung von Schutzschränken

Nach der Beschaffung eines Schutzschrankes (Serverschrank oder Datensicherungsschrank - vgl. auch 11.5.7 Beschaffung und Einsatz geeigneter Schutzschränke) sind die BenutzerInnen in die korrekte Bedienung einzuweisen. Dies sollte auch bei Neuübertragung einer Aufgabe erfolgen, die die Nutzung eines Schutzschrankes umfasst.

Beispiele für zu vermittelnde Punkte sind:

- Korrekter Umgang mit dem Schloss des Schutzschrankes: Dabei ist auf typische Fehler hinzuweisen, wie zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, dass der Schutzschrank bei - auch nur kurzfristiger - Nichtbenutzung verschlossen wird.
- Im Falle eines Serverschrankes ist darauf hinzuweisen, dass unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt werden sollen.
- Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt bzw. bei Bedarf disloziert gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn eine Kopie der Datensicherungsbestände in einem anderen Brandabschnitt bzw. disloziert ausgelagert ist.
- Wird ein klimatisierter Serverschrank eingesetzt, sollten dessen Öffnungszeiten minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

8 Vermögenswerte und Klassifizierung von Informationen

8.1 Vermögenswerte

Unter Vermögenswerten sind gemäß ISO 27002 ganz allgemein zu verstehen:

- Informationen (Daten, Verträge, Vereinbarungen, Dokumentationen, Forschungsergebnisse, Handbücher, Schulungsunterlagen, Verfahrensanleitungen, Pläne, Checklisten, Protokolle, …)
- Software (System-, Anwendungssoftware)
- Gebäude, Einrichtungen, Fahrzeuge, Betriebsmittel, Hardware, Datenträger
- Rechen- und Kommunikationsdienste, Versorgungseinrichtungen
- MitarbeiterInnen mit ihren Qualifikationen und Erfahrungen
- Immaterielle Werte, wie z. B. Ruf und Image der Organisation.

Das heißt vereinfacht: Alles was für eine Organisation einen Wert darstellt. Die folgenden Maßnahmen sollen die Vermögenswerte der Organisation schützen. Dazu ist es zunächst notwendig, sie zu klassifizieren, d. h. zu identifizieren, in einem Verzeichnis aufzulisten, jeweils dazu EigentümerInnen sowie Verantwortliche zu benennen und Regeln für den sicheren Umgang damit aufzustellen.

[Quelle: CASES Leitfaden „Klassifikation“]

8.1.1 Inventar der Vermögenswerte (Assets) mittels Strukturanalyse

Mittels Strukturanalyse werden die Geschäftsprozesse und die dafür benötigten Assets (Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze) erhoben. Zuerst werden geschäftskritische Informationen und Anwendungen ermittelt und die betroffenen IT-Systeme, Räume und Netze erfasst.

Klassische Vorgehensweise ist, zuerst die Anwendungen und ausgehend davon die weiteren betroffenen Objekte zu ermitteln. Allerdings ist es dabei schwierig, abstrakte Anwendungen losgelöst von konkreten technischen Komponenten zu erfassen.

Es kann daher auch zweckmäßig sein, zunächst die IT-Systeme (inklusive vorhandener Industriesteuerungen (ICS) oder Internet-of-Things (IoT)-Komponenten) zu erheben bzw. auf einen bestehenden und aktuellen Netztopologieplan zurückzugreifen. Oft lassen sich dann die Anwendungen anhand der betrachteten IT-Systeme leichter ermitteln.

Eine weitere Vereinfachung des Vorgangs kann sich ergeben, wenn als Datenquellen bereits aktuelle Datenbanken oder Übersichten vorhanden und nutzbar sind (z. B. für die Inventarisierung, das Konfigurationsmanagement oder die Gestaltung von Geschäftsprozessen).

Aktivitäten für eine Strukturanalyse:

- Erfassung der Geschäftsprozesse, Anwendungen und Informationen im Geltungsbereich,
- Erhebung von Datenträgern und Dokumenten,
- Erhebung von IT-, ICS- und IoT-Systemen,
- Netzplanerhebung,
- Erfassung der baulichen Gegebenheiten.

Dabei ist es oft nicht zweckmäßig, jedes Objekt einzeln zu erfassen. Stattdessen sollten Objekte zu Gruppen zusammengefasst werden, wenn sie folgende Ähnlichkeiten aufweisen:

- vom gleichen Typ,
- ähnliche Aufgaben,
- ähnlichen Rahmenbedingungen unterworfen,
- haben den gleichen Schutzbedarf.

Bei technischen Objekten bietet sich in folgenden Fällen eine Gruppierung an:

- ähnlich konfiguriert,
- ähnlich in das Netz eingebunden (z. B. IT-Systeme am gleichen Switch),
- ähnlichen administrativen und infrastrukturellen Rahmenbedingungen unterworfen,
- sie dienen ähnlichen Anwendungen,
- haben den gleichen Schutzbedarf.

Damit wird die Strukturanalyse hinsichtlich Datenmenge und Komplexität handhabbar.

Gruppierung

Bei technischen Komponenten wird durch konsequente Gruppenbildung auch die Administration wesentlich vereinfacht, weil es dann nur wenige Grundkonfigurationen gibt. Durch eine möglichst hohe Standardisierung innerhalb einer IT-Umgebung wird außerdem die Zahl potenzieller Sicherheitslücken reduziert. Eine Stichprobe aus einer Gruppe repräsentiert dann in der Regel den Sicherheitszustand der Gruppe. Sicherheitsmaßnahmen für einen solchen Bereich können ohne Unterscheidung verschiedenster Schwachstellen umgesetzt werden. Überdies können damit auch Kosten gespart werden.

Ein wichtiges Beispiel ist die Zusammenfassung von Clients. In der Regel gibt es in einer Organisation viele Clients, die sich jedoch gemäß obigem Schema in eine überschaubare Anzahl von Gruppen aufteilen lassen (dies gilt analog auch für Räume und andere Objekte oder in Produktionsbetrieben für vergleichbar konfigurierte Geräte wie etwa Handscanner; in großen Informationsverbünden, wo viele Server die gleiche Aufgaben wahrnehmen, können auch Server zu Gruppen zusammengefasst werden).

Gerade auch bei der Verwendung von virtuellen Maschinen (VMs) oder von Systemen bzw. Architekturen aus dem Bereich des Cloud Computings ist eine sinnvolle Strukturanalyse nur durch Gruppenbildung möglich. Besonders trifft dies zu, wenn etwa Geschäftsprozesse über Cloud Computing-Anwendungen ausgelagert werden. Gemäß demselben Prinzip können VMs mit ähnlichen Aufgaben, gleichartig konfiguriert und demselben Schutzbedarf – auch wenn sie auf verschiedenen physischen IT-Systemen laufen – zusammengefasst werden. Bei Cloud Computing-Plattformen ist eine Gruppenbildung unumgänglich und kann beispielsweise anhand des zu identifizierenden Schutzbedarfs durchgeführt werden.

Die Teilaufgaben der Strukturanalyse werden nachfolgend beschrieben. Bei allen Teilaufgaben sollten jeweils Objekte zu Gruppen zusammengefasst werden, wenn dies sinnvoll und zulässig ist.

[Quelle: BSI-Standard 200-2]

8.1.1.1 Erfassung von Geschäftsprozessen, Anwendungen und Informationen

Auf Basis des festgelegten Geltungsbereichs (z.B. gesamte Organisation, Teilbereiche einer Organisation) sind zuerst die wesentlichen Geschäftsprozesse zu erfassen und zu dokumentieren. Wichtig ist hierbei, nicht nur den jeweiligen Hauptprozess zu erfassen, sondern auch die wichtigsten Sub-Prozesse oder Unterstützungsprozesse. Im Produktions- bzw. ICS-Bereich wären dies beispielsweise logistische oder wartungstechnische Nebenprozesse aber auch Beschaffungsprozesse.

Zur Identifizierung von Geschäftsprozessen eignen sich bestehende Geschäftslandkarten, Geschäftsverteilungspläne, Aufgabenbeschreibungen oder andere organisationsbeschreibende Unterlagen. Des Weiteren ist auch das Verfahrensverzeichnis des Datenschutzbeauftragten eine mögliche Quelle für zumindest solche Prozesse, die personenbezogene Daten verarbeiten. Sind keine entsprechenden Prozessunterlagen vorhanden, sollten Interviews oder Workshops mit den jeweiligen Verantwortlichen durchgeführt werden.

Die Erfassung von Geschäftsprozessen sollte jeweils umfassen:

- Eindeutiger Bezeichner
- Name
- Prozessverantwortlicher/Fachabteilung
- Kurze Beschreibung des Prozesses und der verarbeiteten Informationen
- Wichtige, für den Prozess benötigte Anwendungen

Anwendungen dienen der IT-technischen Unterstützung von Geschäftsprozessen in Organisationen (z. B. Behörden, Unternehmen). Ausgehend von jedem Geschäftsprozess im Geltungsbereich sind die damit zusammenhängenden Anwendungen und Informationen zu identifizieren.

Für die geeignete Granularität ist zwischen einerseits einer für die Feststellung des Schutzbedarfs nötige Detaillierung, andererseits der optimalen Effizienz zu optimieren. Abgesehen von der zuvor beschriebenen Gruppenbildung beschränkt sich die Strukturanalyse auf Anwendungen und Informationen, die für die betrachteten Geschäftsprozesse erforderlich sind und jedenfalls ein Mindestniveau an

- Geheimhaltung (Vertraulichkeit) oder
- Korrektheit und Unverfälschtheit (Integrität) oder
- Verfügbarkeit

erfordern.

Um dies sicherzustellen, sollten bei der Erfassung der Anwendungen die BenutzerInnen bzw. die für die Anwendung bzw. für den Geschäftsprozess Verantwortlichen nach ihrer Einschätzung zum erforderlichen Sicherheitsniveau befragt werden - ggf. in gemeinsamen Meetings der Fach-, IT-Abteilungen und Anwendungsverantwortlichen. Denn es ist angesichts der steigenden Komplexität oft schwierig, Abhängigkeiten zwischen Geschäftsprozess und einer konkreten Anwendung darzustellen.

- Es ist also für jeden Geschäftsprozess festzustellen, welche Anwendungen für dessen Abwicklung notwendig sind und auf welche Daten dabei zugegriffen wird.

- Wurden alternativ zuerst die IT-Systeme erfasst, empfiehlt es sich oft, an ihnen orientiert die darauf laufenden Anwendungen zusammenzutragen. Dabei sollte zumeist mit den Servern begonnen werden.
- Ergänzt wird die Erhebung mit den Clients und - mitunter mobilen - Einzelplatzsystemen.
- Schließlich wird noch ermittelt, welche Netzkomponenten welche Anwendungen unterstützen.
- Standard-Software der Clients (z.B. E-Mail- oder Videokonferenzprogramme) sollte als Paket betrachtet werden, um in der Erfassung nicht vergessen zu werden.
- Weiters darf bei der Erfassung auch auf virtualisierte Anwendungen nicht vergessen werden.

Pro erfasster Anwendung:

- Zwecks späterer Zuordnungen sollten die Anwendungen durchnummeriert werden.
- Für Datenschutzbeauftragte/CISOs: Vermerk, ob die beschriebene Anwendung personenbezogene Daten speichert oder verarbeitet (Schutzbedarf der Information ergibt in der Regel Schutzbedarf der Anwendung)
- Unterstützte Geschäftsprozesse
- Verantwortliche und BenutzerInnen der Anwendung (Ansprechpartner für Sicherheitsfragen)

Es empfiehlt sich natürlich eine tabellarische Darstellung bzw. die Nutzung geeigneter Software.

[Quelle: BSI-Standard 200-2]

8.1.1.2 Erfassung von Datenträgern und Dokumenten

Bei der Erfassung der Anwendungen sollten auch Datenträger und Dokumente mitbetrachtet werden, sie können wie Anwendungen behandelt werden. Jedoch sind sie dann gesondert in der Strukturanalyse zu erfassen, wenn sie nicht mit einer bestimmten Anwendung oder einem IT-System verknüpft sind. Auch dafür sollten möglichst Gruppen gebildet und nur Datenträger und Dokumente mit einem Mindestschutzbedarf berücksichtigt werden.

Beispiele für gesondert erfasste Datenträger und Dokumente:

- Archiv- und Backup-Datenträger,
- Datenträger für den Austausch mit externen Kommunikationspartnern,
- Massenspeicher für den mobilen Einsatz (z.B. externe Festplatten oder USB-Sticks),
- Ausgedruckte Notfall- und sonstige Handbücher,

- wichtige Verträge.

Empfehlenswert ist auch die Erfassung der Abhängigkeiten zwischen Anwendungen; so sind beispielsweise Informationen über den Lagerbestand Voraussetzungen für die Verarbeitung von Bestellungen.

[Quelle: BSI-Standard 200-2]

8.1.1.3 Erhebung der IT-Systeme

> *In ebenso tabellarischer Form wird eine Liste der vorhandenen und geplanten IT-Systeme aufgestellt. Der Begriff „IT-System“ umfasst dabei nicht nur Computer im engeren Sinn, sondern auch aktive Netzkomponenten, ICS- und IoT-Geräte, Smartphones, virtuelle IT-Systeme, Netzdrucker, Telekommunikationsanlagen etc. Im Vordergrund steht dabei die technische Realisierung eines IT-Systems, beispielsweise Einzelplatz-PC, Server bzw. Client mit Betriebssystemangabe.*

Allerdings werden Systeme betrachtet und nicht einzelne Bestandteile (CPU, Bildschirm, Tastatur, etc.); es sei denn sie werden im normalen Betrieb mit unterschiedlichen Systemen verbunden (etwa externe Laufwerke). Eine vollständige, korrekte und aktuelle Auflistung der IT-Systeme ist auch für deren Überprüfung, Wartung, Fehlersuche und Instandsetzung notwendig. Zu erfassen sind sowohl die vernetzten als auch die nicht vernetzten IT-Systeme, insbesondere also auch solche, die nicht im Netzplan aufgeführt sind.

Weitere Geräte aus dem ICS- und IoT-Umfeld sind beispielsweise SPS-Steuerungen, Elemente der Gebäudesteuerung, Klimaanlagen, Kaffeemaschinen und weitere nicht unbedingt den Geschäftsprozessen dienende Geräte, die jedoch auch die Informationssicherheit beinträchtigen können. Davon sollten zumindest die vernetzten Geräte erfasst werden, also solche mit Netzwerk-, Internet-, Funk- oder Bluetooth-Verbindung. Solche Geräte sollten möglichst zu Gruppen zusammengefasst werden.

Wurden IT-Systeme im Netzplan zu einer Gruppe zusammengefasst, können sie weiters als ein Objekt behandelt werden, auch solche, die nicht im Netzplan aufgeführt sind (vgl. 8.1.1 Inventar der Vermögenswerte (Assets) mittels Strukturanalyse). Informationen pro IT-System bzw. Gruppe:

- eindeutige Nummerierung, Kürzel oder Bezeichnung des IT-Systems bzw. der jeweiligen Gruppe,
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Beschreibung (z.B. Typ, Funktion),
- Plattform (z. B. Hardwarearchitektur/Betriebssystem, Art der Netzanbindung),
- Aufstellungsort (z. B. Ort, Gebäude, Raum),
- Status (in Betrieb, im Test, in Planung),

- Anwendungen, welche dem IT-System bzw. der Gruppe zuzuordnen sind (Datenverarbeitung oder -transfer),
- BenutzerInnen, AnwenderInnen bzw. AdministratorInnen des IT-Systems.

Auch dafür sollten nach Möglichkeit bereits existierende Datenbanken oder Übersichten über die vorhandenen oder geplanten IT-Systeme genutzt werden. Ergebnis ist eine Übersicht, aus der die Zusammenhänge zwischen den wichtigen Anwendungen und den entsprechenden IT-Systemen hervorgehen.

[Quelle: BSI-Standard 200-2]

8.1.1.4 Netzplan

Ein Netzplan ist eine grafische Übersicht über die im Geltungsbereich eingesetzten Komponenten und deren Vernetzung. Netzpläne oder ähnliche grafische Übersichten sind auch aus betrieblichen Gründen in den meisten Institutionen vorhanden.

Für die Informationssicherheit sind folgende Objekte relevant:

- IT-Systeme (Client- und Server-Computer), aktive Netzkomponenten (wie Switches, Router, WLAN Access Points), Netzdrucker etc.
- ICS- und IoT-Komponenten mit Netzanschluss: Clients, Handscanner, Industriedrucker, Geräte mit speicherprogrammierbarer Steuerung (SPS), Schaltschränke usw.
- Netzverbindungen zwischen diesen Systemen: LANs (Ethernet), WLANs, Backbone-Techniken (ATM) etc.
- Verbindungen nach außen (z. B. Internetzugänge über Modems und Router aber auch Funkstrecken, Mobilfunk sowie Standleitungen zu entfernten Gebäuden oder Liegenschaften etc.

Jedes dargestellte Objekt sollte auch in einem zugehörigen Katalog mit folgenden Elementen eingetragen werden:

- eindeutige Nummerierung, Kürzel oder Bezeichnung als Referenz zur Grafik,
- vollständige Bezeichnung (Hostname, Identifikationsnummer),
- Typ und Funktion (z. B. Datenbank-Server für bestimmte Anwendung Nr. X, …),
- Plattform (Hardware, Betriebssystem),
- Standort (Gebäude-, Raumnummer),
- zuständige AdministratorInnen,
- vorhandene Kommunikationsschnittstellen (z. B. Internet, LAN, WLAN, Bluetooth etc.),
- Art der Netzanbindung und Netzadresse.

Für die Netzverbindungen zwischen den Objekten bzw. nach außen werden Detailinformationen eingetragen, z.B.:

- Art der Verkabelung bzw. Kommunikationsanbindung (z. B. Lichtwellenleiter, verkabeltes LAN, WLAN, 4G, 5G etc.),
- maximale Datenübertragungsrate,
- auf den unteren Schichten verwendete Netzprotokolle (z. B. Ethernet, TCP/IP),
- externe Netzanbindungen (z. B. Internet mit Namen des Providers).

Virtuelle IT-Systeme (z.B. virtuelle Switches, virtuelle Server) und virtuelle Netzverbindungen, wie virtuelle LANs (Virtual Local Area Networks - VLANs) oder virtuelle private Netze (Virtual Private Networks - VPNs), sollten ebenfalls im Netzplan dargestellt werden. Ggf. kann dafür die Aufteilung in separate Teilnetzpläne die Übersichtlichkeit verbessern.

Eine Cloud-Infrastruktur sollte über eine Verwaltungssoftware bzw. Netzmanagement-Tools zur automatischen Erzeugung von Netzplänen verfügen. Im ICS-Bereich, welcher als eigenständiges Netz betrieben wird, sollten auch die Schnittstellen nach außen und insbesondere Internetanbindungen erfasst sowie die Trennung der Netze dargestellt werden.

Es empfiehlt sich, Bereiche mit unterschiedlichem Schutzbedarf zu kennzeichnen.

Der Netzplan sollte möglichst in elektronischer Form mit Hilfe geeigneter Tools erstellt und gepflegt werden.

[Quelle: BSI-Standard 200-2]

8.1.1.5 Erfassung der Gebäude und Räume

In ein Sicherheitskonzept müssen alle Liegenschaften und Gebäude einbezogen werden, innerhalb derer die betrachteten Geschäftsprozesse betrieben werden. Dazu gehören Betriebsgelände, Gebäude, Etagen, Räume sowie die Wegstrecke zwischen diesen.

Viele Organisationen nutzen ein Gebäude oder eine Etage allein, aber häufig nutzen Organisationen Liegenschaften, die weit verstreut sind oder mit anderen Nutzern geteilt werden müssen. Oft sind Geschäftsprozesse auch in fremden oder sporadisch genutzten Räumlichkeiten angesiedelt, beispielsweise für Telearbeitsplätze.

Daher ist es oft sinnvoll, eine je nach Gegebenheiten mehr oder weniger umfangreiche Übersicht bzw. einen Plan über die Liegenschaften, vor allem die Räume, zu erstellen, in denen IT-Systeme aufgestellt oder die für den IT-Betrieb genutzt werden:

- Räume, die ausschließlich dem IT-Betrieb dienen (wie Serverräume, Datenträgerarchive),
- Räume, in denen unter anderem IT-Systeme betrieben werden (wie Büroräume),

- Schutzschränke, in denen IT-Systeme untergebracht sind, sind wie Räume zu erfassen,
- weitere Räume, in denen schutzbedürftige Informationen (Datenträger, aber auch Aktenordner) aufbewahrt werden,
- sowie Wegstrecken, über die Kommunikationsverbindungen laufen.

Dabei sollte auch die Art der in den Räumen jeweils verarbeiteten Informationen nachvollziehbar sein.

[Quelle: BSI-Standard 200-2]

8.1.1.6 Aktualisierung der Strukturanalyse

In der Regel werden die IT- und Netzwerkstrukturen ständig an neue Anforderungen der Organisation angepasst. Nicht in jedem Fall werden solche Änderungen umgehend in den Aufzeichnungen der Erhebung bzw. im Netzplan nachgezogen, da dies meist aufwändig ist. In der Praxis werden oft nur größere Änderungen an der IT-Struktur einzelner Bereiche zum Anlass genommen, den Plan zu aktualisieren. Die Folge ist, dass die Aufzeichnungen dann nicht auf dem aktuellen Stand sind.

Eine häufige Vorgehensweise besteht darin, die vorliegenden Aufzeichnungen periodisch oder anlässlich größerer Änderungen bzw. im Zuge von Audits mit den tatsächlich vorhandenen Strukturen und Objekten abzugleichen und gegebenenfalls auf den neuesten Stand zu bringen:

- Existierende Übersichten, grafische Darstellungen und Netzpläne sichten,
- Diese ggf. aktualisieren oder neu erstellen,
- Existierende Informationen über die enthaltenen IT-, ICS- und IoT-Systeme sichten und gegebenenfalls aktualisieren und vervollständigen,
- Existierende Informationen über die enthaltenen Kommunikationsverbindungen sichten und gegebenenfalls aktualisieren und vervollständigen,
- Existierende Informationen über Liegenschaften, Gebäude und Wegstrecken sichten und gegebenenfalls aktualisieren und vervollständigen.

Dazu sollten auch die IT-Verantwortlichen und AdministratorInnen der einzelnen Anwendungen bzw. Netze konsultiert werden, sowie MitarbeiterInnen der Haustechnik für den Bereich der industriellen Steuerung.

Einige Programme zum zentralisierten Netz- und Systemmanagement unterstützen Objektlisten bzw. Netzpläne, indem sie beispielsweise aktive Komponenten automatisch erkennen. Zu beachten ist jedoch, dass solche Funktionen temporär zusätzlichen Netzverkehr erzeugen. Es muss sichergestellt sein, dass dieser Netzverkehr nicht zu Beeinträchtigungen des IT-Betriebs führt. Ebenso sollte das

Ergebnis von automatischen bzw. halb-automatischen Erkennungen stets daraufhin geprüft werden, ob wirklich alle relevanten Komponenten ermittelt wurden - etwa solche, die sich zum Zeitpunkt des Erkennungslaufes nicht in Betrieb befunden haben.

[Quelle: BSI-Standard 200-2]

8.1.2 Eigentum von Vermögenswerten

Zu jedem Vermögenswert (Asset) muss es eine klar definierte Verantwortlichkeit geben. Dazu wird in der Organisation jedem Vermögenswert bzw. jeder Art von Vermögenswert ein „Eigentümer“ zugewiesen. Dabei ist normalerweise nicht die Eigentümer oder Inhaber im rechtlichen Sinn gemeint, sondern ManagerInnen bzw. Beauftragte, die die Verantwortung für die Verwaltung dieses Vermögenswertes und somit für dessen Sicherheit tragen. Insbesondere sind sie für die Klassifikation des Vermögenswertes und die darauf anzuwendenden Sicherheitsregeln und -maßnahmen verantwortlich. Dazu müssen sie jedoch auch ausreichende und entsprechende Befugnisse besitzen.

Diese Verantwortung kann zwar nicht delegiert werden, aber Eigentümer können MitarbeiterInnen oder BeraterInnen mit der Verwaltung und Ausarbeitung der Regeln beauftragen und genehmigen schließlich die vorgeschlagenen Regeln.

[Quelle: CASES Leitfaden „Klassifikation“]

8.1.2.1 Verantwortliche für Vermögenswerte (Assets)

Grundsätzlich ist die Beteiligung und Mitwirkung aller MitarbeiterInnen einer Organisation an der Umsetzung der erforderlichen Sicherheitsmaßnahmen erforderlich. Dazu müssen sie allerdings wissen, für welche Informationen, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind.

Alle MitarbeiterInnen sind für das verantwortlich, was in ihrem Einflussbereich liegt (es sei denn, es ist explizit anders geregelt). Beispielsweise ist die Leitungsebene der Organisation verantwortlich für alle grundsätzlichen Entscheidungen bei der Einführung einer neuen Anwendung, die Leitung der IT zusammen mit dem Informationssicherheitsmanagement für die Ausarbeitung von Sicherheitsvorgaben für die IT-Komponenten, die AdministratorInnen für deren korrekte Umsetzung und die BenutzerInnen für den sorgfältigen Umgang mit den zugehörigen Informationen, Anwendungen und Systemen.

Es muss jedoch konkret und exakt für alle Informationen, Anwendungen und IT-Komponenten festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Dazu sollte immer eine konkrete Person (inklusive Vertretung) und keine abstrakte Gruppe benannt werden, damit die Zuständigkeit jederzeit deutlich erkennbar ist. Bei komplexeren Informationen, Anwendungen und IT-Komponenten sollten alle Verantwortlichen und deren Vertretungen namentlich genannt sein.

[Quelle: BSI M 2.225]

8.1.2.2 Aufgaben der Eigentümer und Verantwortlichen

Die Fachverantwortlichen als Eigentümer von Informationen und Anwendungen müssen die Sicherheitsmaßnahmen zu deren Schutz sicherstellen, das bedeutet, dass

- *der Schutzbedarf der Informationen, Anwendungen und IT-Komponenten korrekt festgestellt wird,*
- *die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen klar definiert und zugewiesen werden,*
- *die erforderlichen Sicherheitsmaßnahmen umgesetzt werden,*
- *dies regelmäßig überprüft wird,*
- *der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt ist,*
- *die Informationssicherheit gefährdende Abweichungen schriftlich dokumentiert werden.*

Die Fachverantwortlichen müssen zusammen mit dem Management über eine Vorgehensweise befinden, wie mit eventuellen Restrisiken umgegangen werden soll. Die verantwortliche Entscheidung obliegt der Managementebene.

[Quelle: BSI M 2.225]

8.1.3 Zulässige Nutzung von Vermögenswerten

BenutzerInnen von Informationen und die sie verarbeitenden Einrichtungen sind dafür verantwortlich, dass diese nur gemäß ihrer vorgesehenen Bestimmung verwendet und vor Verlust, Diebstahl, Beschädigung, Kompromittierung etc. geschützt werden. Selbstverständlich gehört dazu auch ein generell sorgfältiger und schonender Umgang mit Geräten wie etwa PCs.

Speziell AdministratorInnen und IT-Verantwortliche müssen mit den ihnen eingeräumten, oft weitreichenden Privilegien sorgfältig und nur im vorgesehenen Ausmaß umgehen - dies gilt auch für Notfälle und Ausnahmesituationen.

Bedeutend ist in diesem Zusammenhang auch eine Clear-Desk-Policy, um Kompromittierungen von gedruckten Informationen zu vermeiden.

8.1.3.1 Herausgabe einer PC-Richtlinie

Um einen sicheren und ordnungsgemäßen Einsatz von PCs in größeren Organisationen zu gewährleisten, sollte eine PC-Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Diese PC-Richtlinie soll zumindest den Einsatz von unvernetzten PCs regeln; werden PCs vernetzt betrieben oder als intelligente Terminals genutzt, ist die Richtlinie um diese meist weiter einschränkenden Punkte zu erweitern.

Im Folgenden wird grob umrissen, welche Inhalte für eine solche PC-Richtlinie sinnvoll sind.

Möglicher inhaltlicher Aufbau einer PC-Richtlinie:

- Zielsetzung und Begriffsdefinitionen:
  Dieser erste Teil der PC-Richtlinie soll dazu dienen, die PC-AnwenderInnen für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert und eine einheitliche Sprachregelung geschaffen.
- Geltungsbereich:
  In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt.
- Rechtsvorschriften und interne Regelungen:
  Hier wird auf wichtige Rechtsvorschriften (z. B. das Datenschutzgesetz und das Urheberrechtsgesetz) hingewiesen. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.
- Verantwortungsverteilung:
  In diesem Teil wird definiert, wer im Zusammenhang mit dem PC-Einsatz welche Verantwortung trägt. Dabei sind insbesondere die Funktionen IT-BenutzerInnen, Vorgesetzte, PC-AdministratorInnen, Datenschutzbeauftragte/ CISOs, Informationssicherheitskoordinatoren im Bereichs und Applikations-/ Projektverantwortliche zu unterscheiden.
- Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen:
  Im letzten Teil der PC-Richtlinie ist festzulegen, welche IT-Sicherheitsmaßnahmen von den IT-BenutzerInnen einzuhalten bzw. umzusetzen sind. Es kann je nach Schutzbedarf auch über die IT-Grundschutzmaßnahmen hinausgehen.

Die PC-Richtlinie muss regelmäßig - insbesondere im Hinblick auf die IT-Sicherheitsmaßnahmen - aktualisiert werden.

Es ist dafür Sorge zu tragen, dass alle PC-BenutzerInnen ein Exemplar dieser Richtlinie besitzen und dass die Einhaltung regelmäßig überprüft wird.

Sind TelearbeiterInnen im Unternehmen bzw. in der Behörde beschäftigt, sollte die PC-Richtlinie um die dafür spezifischen Regelungen ergänzt werden. Vgl. dazu 6.3.4 Regelungen für Telearbeit bzw. Homeoffice.

8.1.3.2 Einführung eines PC-Checkheftes

Um die durchgeführten IT-Sicherheitsmaßnahmen am PC zu dokumentieren, kann ein PC-Checkheft eingeführt werden, in dem die PC-NutzerInnen die wichtigsten Angaben zum Gerät dokumentiert. Diese Maßnahme bietet sich in erster Linie für kleine und mittlere Organisationen an, große Organisationen führen und verwalten diese Dokumentationen i. Allg. zentral.

Kommt ein PC-Checkheft zum Einsatz, so sollte es folgende Informationen enthalten:

- Name der PC-Benutzerin bzw. des PC-Benutzers,
- Aufstellungsort des PC,
- Einsatzgebiet (z. B. Kundendienst Inland)
- Erlaubnis (Notebook) aus den Betriebsräumen zu entfernen
- Beschreibung der Konfiguration,
- Zugangsmittel,
- eingesetzte Hard- und Software,
- planmäßige Zeitpunkte für die Datensicherungen,
- durchgeführte Wartungen und Reparaturen,
- durchgeführte Virenkontrollen,
- Zeitpunkt von Passwortänderungen,
- zur Verfügung stehendes Zubehör,
- durchgeführte Revisionen,
- Ansprechpartner für Problemfälle und
- Zeitpunkte der durchgeführten Datensicherungen.

Das Führen eines solchen PC-Checkheftes erleichtert Kontrolltätigkeiten und unterstützt eine notwendige Selbstkontrolle der PC-BenutzerInnen, damit sie regelmäßig Datensicherungen, Passwortänderungen und Viren-Checks durchführen (sofern dies nicht zentral erfolgt (s. o.)).

8.1.3.3 Geeignete Aufbewahrung tragbarer IT-Systeme

Tragbare IT-Systeme wie Notebooks, Netbooks, Tablets oder Smartphones sind durch ihre Bauform immer beliebte Ziele für Diebstähle und müssen sicher aufbewahrt werden - auch dann, wenn sie sich im vermeintlich sicheren Büro befinden. Weil ein tragbares IT-Systeme besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeiten (beispielsweise in einem Schrank oder Schreibtisch) weggeschlossen oder angekettet werden.

Bei mobilem Einsatz müssen die BenutzerInnen versuchen, die tragbaren IT-Systeme auch außer Haus sicher aufzubewahren. Vgl. 6.3.1 Mobile IT-Geräte. Einige Hinweise für die mobile Nutzung:

- Schutz vor Diebstahl und Verlust:
  - Das Gerät sollte gar nicht oder nur in einem minimalen Zeitraum unbeaufsichtigt sein,
  - bei Aufbewahrung eines tragbaren IT-Systems in einem Kraftfahrzeug sollte das Gerät von außen nicht sichtbar sein (Abdecken oder Einschließen in den Kofferraum),
  - jedenfalls sollte das Gerät nur so kurz wie möglich in einem Kraftfahrzeug aufbewahrt werden (keinesfalls über Nacht),
  - wird das mobile IT-System in einem fremden Büro vor Ort benutzt, so ist entweder dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen oder das Gerät mitzunehmen. Zusätzlich ist ein Zugriffschutz zu aktivieren oder das Gerät auszuschalten, um unerlaubte Nutzung zu verhindern,
  - in Hotelzimmern sollte das mobile IT-System nicht offen herumliegen, sondern in einem Schrank verschlossen werden.
  - Bietet das Gerät eine Möglichkeit zum Anketten, sollte sie wo möglich genutzt werden.
  - Zur Beaufsichtigung des Geräts gehört auch, es nicht etwa im Taxi, am Flughafen, im Flugzeug oder im Hotelzimmer zu vergessen.
- Schutz vor Beschädigung:
  - Ein mobiles IT-System sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können anderenfalls beschädigt werden. Auch deshalb sollten IT-Geräte (aber auch ihre Akkus) nicht in geparkten Autos zurückgelassen werden.
  - Ebenso sollten mobile Endgeräte vor schädlichen Umwelteinflüssen geschützt werden, also beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.

- Mobile IT-Systeme sind heute zwar robust, aber dennoch sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. Bei Notebooks sollte beispielsweise das Gerät zusammengeklappt werden, da sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich ist es immer empfehlenswert, für den Transport ein schützendes Behältnis zu verwenden.

Es ist empfehlenswert, für die BenutzerInnen mobiler IT-Systeme ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen zur geeigneten Aufbewahrung und zum sicheren Transport der Geräte enthält.

[Quelle: BSI M 1.33, M 1.34]

8.1.3.4 Mitnahme von Datenträgern und IT-Komponenten

Datenträger und IT-Komponenten sind meist innerhalb der Liegenschaft(en) der eigenen Organisation hinreichend vor Missbrauch und Diebstahl geschützt. Oft sollen sie aber auch außer Haus eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Für einen ausreichenden Schutz muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten bzw. Datenträger außer Haus mitnehmen darf,
- welche grundlegenden IT-Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung sensitiver Daten, Aufbewahrung etc.).

Die Art und der Umfang der anzuwendenden IT-Sicherheitsmaßnahmen für extern eingesetzte IT-Komponenten hängt einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden müssen.

Gibt es (z. B. in größeren Organisationen) Zutrittskontrollen durch Portier- oder Wachdienste, kann mittels Stichproben kontrolliert werden, inwieweit die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden. Dabei ist jedoch darauf zu achten, dass solche Kontrollen nicht in unnötig schikanöse Durchsuchungen ausarten.

Außerhalb der organisationseigenen Büros bzw. Liegenschaften sind die BenutzerInnen für den Schutz der ihnen anvertrauten IT verantwortlich und darauf sowie auf zu ergreifende Vorsichtsmaßnahmen sind sie hinzuweisen, etwa:

- IT-Systeme müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt bleiben oder in Fahrzeugen zurückgelassen werden (siehe auch 8.1.3.3 Geeignete Aufbewahrung tragbarer IT-Systeme).
- IT-Systeme wie Notebooks oder Mobiltelefone und deren Anwendungen können i. Allg. durch PINs, Passwörter oder anderen Mechanismen abgesichert werden. Diese sollten auch genutzt werden.
- IT-Systeme oder Datenträger, die sensitive Daten enthalten, sollten möglichst komplett verschlüsselt werden.
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten IT-Systemen sollte geregelt werden.
- Es sollte protokolliert werden, wann und von wem welche IT-Komponenten außer Haus eingesetzt wurden.
- Bei Mitnahme ins Ausland ist zu beachten, ob es ein unerlaubter Import von Verschlüsselungstechnik sein könnte.
- Es ist mit der Offenlegung der Daten vor Zollbeamten zu rechnen.

[Quelle: BSI M 1.218]

8.1.3.5 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Videokameras

Das Mikrofon bzw. die Videokamera eines vernetzten Rechners kann von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei haben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand an dem IT-System arbeitet. Wenn die Benutzung eines vorhandenen Mikrofons oder einer Kamera generell verhindert werden soll, müssen diese - wenn möglich - ausgeschaltet oder physikalisch vom Gerät getrennt werden bzw. die Kamera überklebt werden.

Falls das Mikrofon bzw. die Kamera in den Rechner (bzw. den Bildschirm) integriert ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, dass es keine Unbefugten benutzen können.

Es ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, dass alle BenutzerInnen das Mikrofon bzw. die Kamera benutzen können (und nicht nur in Einzelfällen eine Freigabe durch die SystemadministratorInnen erfolgen soll), muss die Systemadministration ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diese BenutzerInnen aktiviert werden kann und
- die Zugriffsberechtigungen den BenutzerInnen nach dem Abmelden wieder entzieht.

Wünschenswert wäre es auch, Mikrofon und Kamera nach einer voreingestellten Zeitspanne ohne Aktivität automatisch abzuschalten (Timeout).

8.1.3.6 Absicherung von Wechselmedien

Wechselmedien, wie etwa USB-Sticks, USB-Festplatten, SD-Karten etc., ermöglichen raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Als derartige Risiken wären unter anderem zu nennen:

- unkontrolliertes Booten von Geräten etwa von USB-Sticks, USB-Festplatten oder DVD-ROM,
- unautorisierte Installation von Software und
- unberechtigte Kopien von Daten auf Wechselmedien (Verlust der Vertraulichkeit).

Zur Verringerung dieser Bedrohungen stehen - abhängig von der Art der Wechselmedien und dem zugrunde liegenden Betriebssystem - eine Reihe von Möglichkeiten zur Verfügung, die unten beispielhaft angeführt werden. Es ist aber zu betonen, dass in vielen Fällen eine völlige Sperre der Wechselmedien entweder technisch nicht möglich oder aber aus betrieblichen Gründen nicht durchsetzbar ist. Hier sind zusätzliche personelle (Anweisungen, Verbote, …) und organisatorische Maßnahmen (Kontrollen, …) erforderlich.

Maßnahmen zur Sicherung von Wechselmedien:

- Verzicht auf USB-, DVD-ROM-, …, Laufwerke (bzw. ihr nachträglicher Ausbau)
- (Physischer) Verschluss von Laufwerken (z. B. durch Einsatz von Schlössern).
- (Logische) Sperre von Schnittstellen:
  Viele Betriebssysteme bieten die Möglichkeit, Schnittstellen zu sperren. Dabei ist allerdings zu beachten, dass dies nicht immer technisch möglich und oft auch aus betrieblichen Gründen nicht durchführbar ist.
- Deaktivierung im BIOS/UEFI:
  Das BIOS (Basic Input/Output System) bzw. UEFI (Unified Extensible Firmware Interface) bieten Möglichkeiten um nur von bestimmten Laufwerken zu booten. Es muss jedoch auch sichergestellt werden, dass die BenutzerInnen diese Einstellungen nicht mehr verändern können.
- Verschlüsselung:
  Es existieren verschiedenste Produkte, die Zugriffe ausschließlich auf Datenträger, die mit bestimmten kryptografischen Schlüsseln versehen worden sind, zulassen.
- Regeln:

In vielen Fällen ist die Benutzung externer Speichermedien durchaus erlaubt, jedoch bestimmten Regeln unterworfen. Es sollte hierbei jedenfalls das Booten von Wechselmedien im BIOS bzw. UEFI deaktiviert werden. Solche Regeln könnten etwa Beschränkungen auf die Verwendung bestimmter Dateitypen sein. Die jeweiligen Regeln müssen allen BenutzerInnen bekannt gegeben werden und deren Einhaltung kontrolliert werden.

- Gegebenenfalls Verblenden und Verplomben von Schnittstellen
  Nach Anschluss aller erforderlichen Schnittstellen wird die Rückseite des Gerätes mit einer speziellen Abdeckung verblendet. Diese wird verplombt, so dass etwaige Manipulationen ersichtlich sind. Diese Vorgehensweise bietet einen relativ hohen Grad an Sicherheit (insbesondere an nachträglichen Nachweismöglichkeiten), es ist aber zu bedenken, dass damit die Flexibilität der Systeme stark eingeschränkt wird. Häufige Übersiedlungen, Konfigurationsänderungen etc. können die Akzeptanz dieser Maßnahme bei BenutzerInnen und Systemverantwortlichen stark reduzieren.

Es ist auch zu bedenken, dass bei IT-Systemen im Netzwerk ein Laden von Treibern etc. etwa über das Internet oder mittels Attachments von E-Mails möglich ist. Hier sind entsprechende Vorkehrungen zu treffen. Vgl. 6.3.1.3 Wechselmedien und externe Datenspeicher.

8.2 Klassifizierung von Informationen

Die Klassifizierung der verarbeiteten, gespeicherten und übertragenen Informationen in Bezug auf ihre Vertraulichkeit und die Datenschutzanforderungen ist wesentliche Voraussetzung für die spätere Auswahl adäquater Sicherheitsmaßnahmen.

Daher sind in der Informationssicherheitspolitik entsprechende Sicherheitsklassen zu definieren und weiters die Verantwortlichkeiten für die Durchführung der Klassifizierung festzulegen.

8.2.1 Definition der Sicherheitsklassen

Festlegung von Klassifizierungsstufen bzgl. Vertraulichkeit (Vertraulichkeitsklassen)

Die Vertraulichkeitsklassen können als Maß dafür gesehen werden, welche Auswirkungen ein Missbrauch der Information auf die Institution haben kann.

Im Bereich der Bundesverwaltung sind die unten angeführten hierarchischen Klassen definiert. Diese Klassen sind lt. Informationssicherheitsgesetz gesetzlich festgelegt für „klassifizierte Informationen, die Österreich im Einklang mit völkerrechtlichen Regelungen erhalten hat“.

HINWEIS: Im Sinne der Kompatibilität und Einheitlichkeit erscheint diese Klassifizierung auch für andere Daten im Bereich der Bundesverwaltung sinnvoll.

- EINGESCHRÄNKT:
  Die unbefugte Weitergabe der Informationen würde den in Art. 20, Abs. 3 B-VG genannten Interessen zuwiderlaufen. [Anmerkung: Alle mit Aufgaben der Bundes-, Landes- und Gemeindeverwaltung betrauten Organe sowie die Organe anderer Körperschaften des öffentlichen Rechts sind, soweit gesetzlich nicht anderes bestimmt ist, zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordenen Tatsachen verpflichtet, deren Geheimhaltung im Interesse der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen, im wirtschaftlichen Interesse einer Körperschaft des öffentlichen Rechts, zur Vorbereitung einer Entscheidung oder im überwiegenden Interesse der Parteien geboten ist (Amtsverschwiegenheit), …]
- VERTRAULICH:
  Die Informationen stehen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz und ihre Geheimhaltung ist im öffentlichen Interesse gelegen.
- GEHEIM:
  Die Informationen sind vertraulich und ihre Preisgabe würde zudem die Gefahr einer erheblichen Schädigung der in Art. 20, Abs. 3 B-VG genannten Interessen schaffen.
- STRENG GEHEIM:
  Die Informationen sind geheim und ihr Bekanntwerden würde überdies eine schwere Schädigung der in Art. 20, Abs. 3 B-VG genannten Interessen wahrscheinlich machen.

Nicht-klassifizierte Informationen werden nachfolgend auch als „offen“ bezeichnet.

In den übrigen Verwaltungsbereichen und in der Privatwirtschaft ist es jeder Organisation überlassen, in ihrer Informationssicherheitspolitik eine für ihre Zwecke adäquate Definition von Vertraulichkeitsklassen vorzunehmen, sofern es nicht bereits diesbezügliche Regelungen gibt. Aus Gründen der Kompatibilität wird die Anwendung des genannten Schemas in denjenigen Bereichen, in denen nicht zwingende Gründe für ein anderes Klassifizierungsschema bestehen, empfohlen. Allerdings werden Organisationen der Privatwirtschaft, sofern sie nicht besonders strenge Sicherheitsanforderungen haben, i. Allg. mit weniger Klassen (meist 3 oder 4) das Auslangen finden.

Im Rahmen der Informationssicherheitspolitik sollte darauf hingewiesen werden, dass die Klassifizierung der Daten sehr sorgfältig vorzunehmen ist. Nicht nur die Einstufung in eine zu niedrige Vertraulichkeitsklasse ist mit potenziellen Gefahren verbunden, auch die leichtfertige Einstufung in eine zu hohe Vertraulichkeitsklasse ist zu vermeiden, da etwa die Behandlung von geheimen Daten durchwegs mit erheblichem Aufwand verbunden ist.

Klassifizierung von Daten in Bezug auf Datenschutz

Werden personenbezogene Daten verarbeitet, so sind die Daten auch dahingehend zu klassifizieren. Die nachfolgende Klassifizierung gemäß Datenschutzgesetz (DSG) gilt sowohl für den Behörden- als auch für den privatwirtschaftlichen Bereich.

- ANONYM:
  Daten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Achtung: pseudonymisierte Daten zählen hierzu nicht!
- PERSONENBEZOGEN:
  Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Weiters fallen in diese Klassifizierungsstufe auch pseudonymisierte Daten, also solche personenbezogenen Daten, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Der Schutz dieser pseudonymisierten Daten und die Aufrechterhaltung der Trennung gegenüber zuordenbaren Informationen erfordern jedoch ein ebenbürtiges Niveau zu personenbezogenen Daten, damit nicht unrechtmäßiger Weise wieder ein Personenbezug hergestellt werden kann. Pseudonymisierte Daten sollten daher in dieser Hinsicht wie personenbezogene Daten klassifiziert werden.
- SENSIBEL (besondere Kategorien personenbezogener Daten):
  Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

8.2.2 Festlegung der Verantwortlichkeiten und der Vorgehensweise für klassifizierte Informationen

Im Rahmen der Informationssicherheitspolitik ist generell festzulegen, wer die Klassifizierung der Daten vorzunehmen hat. Dies kann in den einzelnen Organisationen unterschiedlich sein und auch von IT-System zu IT-System differieren.

Als allgemeine Richtlinie kann gelten, dass die Klassifizierung einer Information von jener Person vorzunehmen ist, von der diese Information stammt, oder, wenn diese keine eindeutigen Vorgaben gemacht hat, von jener Person in der Organisation, die diese Information von außen erhält.

Weiters ist festzulegen, in welcher Form die Klassifizierung bzw. Deklassifizierung erfolgt und wie klassifizierte Information gekennzeichnet wird.

Die für die Information verantwortlichen MitarbeiterInnen werden oft als „Dateneigner“ oder „Data Owner“ bezeichnet.

8.2.3 Erarbeitung von Regelungen zum Umgang mit klassifizierten Informationen

In diesem Schritt ist festzulegen, wie die Information in Abhängigkeit von den Sicherheitsklassen zu behandeln ist.

Werden in einer Organisation häufig klassifizierte Informationen verarbeitet und gespeichert, so empfiehlt sich die Erarbeitung eines eigenständigen Dokumentes, in dem u. a. folgende Fragen behandelt werden:

- Kennzeichnung klassifizierter Information (sowohl elektronischer als auch nicht elektronischer)
- Verwahrung klassifizierter Information (Zugriffsberechtigungen, etwaige Vorschriften zur Verschlüsselung)
- Übermittlung klassifizierter Information (mündliche Weitergabe, persönliche Weitergabe, Versendung durch Post oder Kurier, elektronische Übertragung, über welche Verbindungen, Vorschriften zur Verschlüsselung)
- Registrierung klassifizierter Information
- Ausdruck klassifizierter Information (auf welchem Drucker, durch wen)
- Backup (Klartext, chiffriert, Schutz der Backup-Medien)
- Aufbewahrung/Wiederverwendung/Vernichtung von Datenträgern mit klassifizierter Information
- Weitergabe klassifizierter Information (an wen, durch wen, unter welchen Bedingungen)
- Deklassifizierung klassifizierter Information (wann, durch wen)

8.2.4 Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung

Ziel der Business Continuity-Planung ist es, die Verfügbarkeit der wichtigsten Applikationen und Systeme innerhalb eines definierten Zeitraumes zu gewährleisten sowie Vorkehrungen zur Schadensbegrenzung im Katastrophenfall zu treffen („Gewährleistung eines kontinuierlichen Geschäftsbetriebes“).

Dabei wird unterschieden zwischen der Aufrechterhaltung der Betriebsverfügbarkeit im Fall von Störungen oder Bedienungsfehlern (im Folgenden auch als „Business Contingency-Planung“ bezeichnet) sowie der Gewährleistung eines Notbetriebes und des geordneten Wiederanlaufs im Katastrophenfall (Katastrophenvorsorge, K-Planung).

Im Rahmen der Informationssicherheitspolitik sind die Verfügbarkeitsklassen für IT-Anwendungen und die diesen Anwendungen zugrunde liegenden IT-Systeme sowie der darauf verarbeiteten oder gespeicherten Informationen zu definieren. Die Business Continuity-Planung selbst ist nicht Bestandteil der Informationssicherheitspolitik, sondern muss in den entsprechenden weiteren Aktivitäten erfolgen.

Nachfolgend ein Beispiel für ein solches Klassifizierungsschema – basierend auf den Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich des Bundeskanzleramtes [K-Fall]:

- **Betriebsverfügbarkeitskategorie 1 – Keine Vorsorge (unkritisch):**
  Für die IT-Anwendung werden keine besonderen Vorkehrungen getroffen. Es ist ein Datenverlust bzw. Ausfall der IT-Anwendung unbestimmter Dauer denkbar. Eine Behinderung in der Wahrnehmung der Aufgaben der betroffenen Verwaltungsstelle entsteht durch den Ausfall bzw. Datenverlust nicht.
- **Betriebsverfügbarkeitskategorie 2 – Offline Sicherung:**
  Es sind die gängigen Sicherungsmaßnahmen für die IT-Anwendung vorgesehen, ein Datenverlust ist auszuschließen. Die IT-Anwendung kann bei technischen Problemen erst nach deren Behebung am ursprünglichen Produktivsystem in Betrieb genommen werden. Die Sicherung wird an einen externen Ort ausgelagert.
- **Betriebsverfügbarkeitskategorie 3 – Redundante Infrastruktur:**
  Die Infrastruktur für die IT-Anwendung ist derart ausgelegt, dass bei Ausfall einer IT-Komponente der Betrieb durch redundante Auslegung ohne Unterbrechung fortgesetzt werden kann.
- **Betriebsverfügbarkeitskategorie 4 – Redundante Standorte:**
  Die IT-Infrastruktur sowie die darauf aufsetzende IT-Anwendung ist auf zwei Standorte verteilt, so dass bei Betriebsunterbrechung des einen Standortes die IT-Anwendung uneingeschränkt am zweiten Standort weiter betrieben werden kann.

Zusätzlich zu den vier genannten Kategorien ist noch die Zusatzqualität „K-Fall sicher“ definiert, welche auch die Anforderungen in Katastrophenfällen berücksichtigt:

- **K-Fall sicher (K2 bis K4):**
  Die IT-Anwendung ist derart konzipiert, dass zumindest ein Notbetrieb in einer Zero-Risk-Umgebung möglich ist. Dazu werden die Daten je nach Aktualisierungsgrad laufend in die Zero-Risk-Umgebung transferiert und der Betrieb der IT-Anwendung derart gestaltet, dass ein Wiederaufsetzen eines definierten Notbetriebes in der Zero-Risk-Umgebung umgehend möglich ist.

In Summe ergibt eine derartige Einstufung die Verfügbarkeitsklassen 1 bis 4 und K2 bis K4. Die Zusatzoption „K-Fall sicher“ in Verbindung mit Betriebsverfügbarkeitskategorie 1 ist nicht sinnvoll.

Für nähere Informationen und für Klassifizierungsbeispiele siehe 17.1.1 Definition von Verfügbarkeitsklassen

8.3 Betriebsmittel und Datenträger

In diesem Kapitel werden generelle Richtlinien zum Umgang mit Betriebsmitteln und Datenträgern gegeben. Der Umgang mit Datenträgern und den darauf gespeicherten Informationen ist in der „Informationssicherheitspolitik“ einer Organisation festzulegen (vgl. dazu 8.2 Klassifizierung von Informationen). Diese Klassifikation und die damit verbundene Festlegung der Verantwortlichkeiten und Vorgehensweisen stellen eine wesentliche Grundlage für die IT-Sicherheit einer Organisation dar.

Insbesondere sei darauf hingewiesen, dass einerseits die Klassifizierung der Daten national durch das Datenschutzgesetz sowie durch das Informationssicherheitsgesetz geregelt wird. International bzw. im EU-Raum ist der „Beschluss des Rates vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates“ (2001/264/EG) einzuhalten, der die Verbindung zwischen den nationalen Klassifizierungen und Richtlinien darstellt. Dies ist gegebenenfalls in der Informationssicherheitspolitik zu berücksichtigen.

8.3.1 Betriebsmittelverwaltung

Betriebsmittel für den IT-Einsatz sind alle erforderlichen Mittel wie Hardwarekomponenten (Rechner, Tastatur, Drucker, …), Software (Systemsoftware, Individualprogramme, Standardsoftware u. ä.), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Festplatten, Wechselplatten, DVD-ROMs u. ä.).

Die Betriebsmittelverwaltung umfasst folgende Aufgaben:

- Beschaffung,

- Prüfung vor Einsatz,
- Kennzeichnung,
- Bestandsführung und
- Außerbetriebnahme.

Beschaffung:

Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden. Eine zentrale Beschaffung sichert auch die Einführung und Einhaltung eines „Hausstandards“ und vereinfacht damit die Schulung der MitarbeiterInnen und die Wartung.

Prüfverfahren vor Einsatz:

Mit einem geregelten Prüfverfahren vor Einsatz der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden.

Beispiele dafür sind:

- Überprüfung der Vollständigkeit von Lieferungen (z. B. Handbücher), um die Verfügbarkeit aller Lieferteile zu gewährleisten,
- Test neuer PC-Software sowie neuer vorformatierter Datenträger mit einem Virensuchprogramm,
- Testläufe neuer Software auf speziellen Testsystemen,
- Überprüfung der Kompatibilität neuer Hardware- und Softwarekomponenten mit den vorhandenen.

Bestandsführung:

Alle wesentlichen Betriebsmittel sollten mit eindeutigen Identifizierungsmerkmalen gekennzeichnet werden. Zusätzlich sollten die Seriennummern vorhandener Geräte wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.

Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muss Auskunft geben können über Identifizierungsmerkmale, Beschaffungsquellen, Lieferzeiten, Verbleib der Betriebsmittel, Lagerhaltung, Aushändigungsvorschriften, Wartungsverträge und Wartungsintervalle.

Eine ordnungsgemäße Bestandsführung erleichtert nicht nur die Verbrauchsermittlung und Veranlassung von Nachbestellungen, sondern ermöglicht auch Vollständigkeitskontrollen, die Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln.

Im Bundesbereich gibt es Vorschriften über die Bestandsführung, die „Richtlinien für die Inventar- und Materialverwaltung (RIM)“. Die dort vorgesehenen Aufzeichnungen reichen aber für einen sicheren EDV-Betrieb nicht aus. Die für den sicheren Betrieb zuständige Organisationseinheit muss daher eigene, entsprechend erweiterte Aufzeichnungen führen.

8.3.2 Datenträgerverwaltung

Die Datenträgerverwaltung stellt einen Teil der Betriebsmittelverwaltung dar. Ihre Aufgabe ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit zu gewährleisten.

Neben den in 8.3.1 Betriebsmittelverwaltung angeführten Maßnahmen ist für die Verwaltung von Datenträgern zusätzlich zu beachten:

- Die äußerliche Kennzeichnung von Datenträgern soll deren schnelle Identifizierung ermöglichen, jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Datenträgers mit dem Stichwort „Gehaltsdaten“), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.
- Für eine sachgerechte Behandlung von Datenträgern sind die Herstellerangaben zu beachten.
- Hinsichtlich der Aufbewahrung von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.
- Versand und Transport: Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten. Hier sind die in der Informationssicherheitspolitik festzulegenden Regeln umzusetzen (etwa Versand nur in verschlossenen/versiegelten Behältnissen, durch Kurierdienst, in chiffrierter Form etc.).
- Der Datenträger darf über die zu versendenden Daten hinaus keine „Restdaten“ enthalten. Dies kann durch physikalisches Löschen erreicht werden (siehe auch unten „Wiederaufbereitung“).
- Vor Versand oder Weitergabe wichtiger Datenträger sollte eine Sicherungskopie erstellt werden. Das Anfertigen von Kopien ist zu dokumentieren und die Kopien sind als solche zu kennzeichnen.
- Wiederaufbereitung:
  Eine geregelte Vorgehensweise für die Löschung bzw. Wiederaufbereitung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern, die schutzwürdige Daten enthalten haben, müssen diese Daten in irreversibler Form gelöscht werden.

- Außerbetriebnahme, Reparaturtausch: Datenträger, die schutzwürdige Daten enthalten und außer Betrieb genommen oder im Zuge einer Reparatur ausgetauscht werden sollen, sind mechanisch zu zerstören (vgl. dazu auch ÖNORM S 2109 Akten- und Datenvernichtung sowie 14.6 Wartung).

Für den Fall, dass von Dritten erhaltene Datenträger eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Viren zu überprüfen. Vgl. dazu auch 12.3 Schutz vor Schadprogrammen und Schadfunktionen.

8.3.3 Datenträgeraustausch

Kennzeichnung der Datenträger beim Versand

Neben den in 8.3.2 Datenträgerverwaltung dargestellten Umsetzungshinweisen ist bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern darauf zu achten, dass AbsenderIn und (alle) EmpfängerInnen unmittelbar zu identifizieren sind. Die Kennzeichnung muss den Inhalt des Datenträgers eindeutig für die EmpfängerInnen erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, dass diese Kennzeichnung für Unbefugte nicht interpretierbar ist.

Darüber hinaus sollten die Datenträger mit den für das Auslesen notwendigen Parametern gekennzeichnet werden. Das Versanddatum, eventuelle Versionsnummern oder Ordnungsmerkmale können gegebenenfalls nützlich sein.

Regelung des Datenträgeraustausches

Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch einige Punkte zu beachten.

Zum Beispiel:

- Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollte neben dem Namen der Empfängerin bzw. des Empfängers auch die Organisationseinheit und die genaue Bezeichnung der Behörde/ des Unternehmens angegeben sein. Entsprechendes gilt für die Adresse der Absenderin/des Absenders.

- Dem Datenträger sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der AbsenderIn, EmpfängerIn, Art des Datenträgers, Seriennummer, Identifikationsmerkmale für den Inhalt des Datenträgers, Datum des Versandes, ggf. Datum bis wann der Datenträger spätestens die EmpfängerInnen erreicht haben muss, sowie Parameter, die zum Lesen der Informationen benötigt werden, enthält.
- Bei regelmäßigem Austausch von Datenträgern zwischen den gleichen Partnern empfiehlt es sich, dafür stets die gleichen Datenträger zu verwenden, so dass bei einem evtl. Fehler bei der Wiederaufbereitung (vgl. 8.3.2 Datenträgerverwaltung) die potenziellen Auswirkungen möglichst gering gehalten werden.
- Abhängig von den Regelungen der Informationssicherheitspolitik sind Datenträger, die Daten hoher Vertraulichkeitsstufen enthalten, beim Transport durch Dritte entweder zu verschlüsseln, oder in entsprechend versperrten Behältnissen zu transportieren

Nicht vermerkt werden sollte,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde,
- welchen Inhalt der Datenträger hat.

Der Versand des Datenträgers kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Je nach Schutzbedarf beziehungsweise Wichtigkeit der übermittelten Informationen ist der Empfang zu quittieren und ein Quittungsvermerk dem erwähnten Protokoll beizufügen.

Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen.

9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung

9.1 Zugriffskontrollpolitik

Durch organisatorische und technische Vorkehrungen ist sicherzustellen, dass der Zugriff zu IT-Systemen, Netzwerken, Programmen und Daten nur berechtigten Personen oder Prozessen und nur im Rahmen der festgelegten Regeln möglich ist.

9.1.1 Grundsätzliche Festlegungen zur Rechteverwaltung

Folgende grundsätzliche Festlegungen zur Rechteverwaltung in einem IT-System sollten - vorzugsweise im Rahmen der IT-Systemsicherheitspolitik - getroffen werden („Zugriffskontrollpolitik“):

- welche Subjekte (z. B. Personen, Programme, Prozesse, …) und welche Objekte (z. B. IT-Anwendungen, Daten, …) unterliegen der Rechteverwaltung,
- welche Arten von Rechten (z. B. Lesen, Schreiben, Ausführen, …) können zwischen Subjekten und Objekten existieren,
- wer darf Rechte einsehen, vergeben bzw. ändern,
- welche Regeln müssen bei Vergabe bzw. Änderung eingehalten werden (Authentisierung, evtl. 4-Augen-Prinzip),
- welche Rollen müssen durch die Rechteverwaltung definiert werden (z. B. AdministratorInnen, Revision, BenutzerInnen, …),
- welche Rollen sind miteinander unvereinbar (z. B. BenutzerIn und Revision, AdministratorIn und AuditorIn, …),
- wie erfolgen Identifikation und Authentisierung.

Die Rechteverwaltung muss vollständig, widerspruchsfrei und überschaubar sein.

Umgesetzt werden die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Definition von Rollen

Viele IT-Systeme lassen es zu, Rollen zu definieren, denen bestimmte Rechte zugeordnet werden. Solche Rollen können etwa sein: AdministratorIn, DatensichererIn, DatenerfasserIn oder SachbearbeiterIn.

9.2 Benutzerverwaltung

Wesentlich sind Verfahren zur geordneten und dokumentierten Erteilung von Zugriffsrechten auf Informationssysteme. Diese sollen über die gesamte Lebensdauer des Zugriffsrechtes wirken, also vom erstmaligen Einrichten neuer BenutzerInnen bis zur Entfernung, wenn kein Zugriff mehr benötigt wird. Besonders relevant ist dabei die Kontrolle über privilegierte Zugriffsrechte, da damit Systemkontrollen außer Kraft gesetzt werden können.

Dies umfasst

- die Dokumentation der zugelassenen BenutzerInnen und zugehöriger Rechteprofile,
- das Einrichten der Zugriffsrechte,
- das Erarbeiten von Richtlinien für die Zugriffs- bzw. Zugangskontrolle,
- die geeignete Auswahl von Authentikationsmechanismen,
- den sicherer Umgang mit IDs und Passwörtern und
- die Aufteilung von Administratortätigkeiten.

9.2.1 Vergabe und Verwaltung von Zugriffsrechten

Die Vergabe und Verwaltung von Zugriffsrechten wird in hohem Maße vom spezifischen IT-System, den darauf durchgeführten Aufgaben sowie der betroffenen Organisation abhängig sein.

Es gibt jedoch einige Grundregeln, deren Einhaltung generell empfohlen wird:

- Die Rechteverwaltung darf nur durch Berechtigte und nur im Rahmen der in der Zugriffskontrollpolitik festgelegten Regeln durchgeführt werden.
- Grundsätzlich sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“).
- Alle BenutzerInnen sollten ihre Rechte innerhalb einer Anwendung einsehen können, ebenso alle Verantwortlichen für ihren Bereich.
- Personelle und aufgabenbezogene Änderungen müssen innerhalb der Rechteverwaltung unverzüglich berücksichtigt werden.
- Es muss ein geregeltes Verfahren für den temporären Entzug von Zugriffsrechten (z. B. bei Urlaub, Karenz, …) bestehen.
- Bei Ausscheiden von MitarbeiterInnen sind deren Kennung und die zugehörigen Rechte unverzüglich zu deaktivieren bzw. zu löschen.
- Nicht mehr aktive Benutzerkennungen dürfen nicht für NachfolgerInnen reaktiviert werden.

- Zusätzlich sollte in definierten Abständen eine Suche nach „toten Benutzerkennungen“, also Kennungen, die seit einem längeren, systembezogen zu definierenden Zeitraum nicht benutzt wurden, vorgesehen sein.

9.2.2 Einrichtung und Dokumentation der zugelassenen BenutzerInnen und Rechteprofile

Regelungen für die Einrichtung von BenutzerInnen bzw. Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.

Es sollte ein Formblatt existieren, um von allen BenutzerInnen bzw. für jede Benutzergruppe zunächst die erforderlichen Daten zu erfassen, z. B.:

- Name, Vorname, eindeutige Identifikation zumindest des jeweiligen Berechtigungssystems,
- Vorschlag für die BenutzerInnen- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,
- Erreichbarkeit (z. B. Telefon, Raum, …),
- ggf. Projekt,
- ggf. Angaben über die geplante Tätigkeit im System und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Passwörter, die neuen BenutzerInnen für die erstmalige Systemnutzung mitgeteilt werden, müssen danach gewechselt werden (siehe auch 9.3.1 Regelungen des Passwortgebrauches). Dies sollte vom System initiiert werden.

Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen, wie zum Beispiel eine Kombination aus Vor- und Nachnamen (z. B. vorname.nachname) oder eigene Benutzer-IDs (z. B. Kürzel der Organisationseinheit plus laufende Nummer).

Anonymisierte bzw. generische Benutzerkennungen sind nur bei unbedenklichen Inhalten, die jedoch nicht öffentlich, sondern einem eingeschränkten Benutzerkreis zugänglich sein sollen, zulässig.

Für sensible IT-Systeme bzw. Anwendungen, bei denen personenbezogene Zugriffssicherheit erforderlich ist, müssen allen BenutzerInnen eigene Benutzerkennungen zugeordnet sein, es dürfen nicht mehrere BenutzerInnen unter derselben Kennung arbeiten.

Dokumentation

Die Dokumentation dient der Übersicht über die zugelassenen BenutzerInnen, Benutzergruppen und Rechteprofile und ist Voraussetzung für Kontrollen.

Dokumentiert werden sollen insbesondere

- die zugelassenen BenutzerInnen mit folgenden Mindestangaben: zugeordnetes Rechteprofil (ggf. Abweichungen vom verwendeten Standard-Rechteprofil), Begründung für die Wahl des Rechteprofils (und ggf. der Abweichungen), Erreichbarkeit der BenutzerInnen, Zeitpunkt und Grund der Einrichtung und Befristungen sowie
- die zugelassenen Gruppen mit den zugehörigen BenutzerInnen, Zeitpunkt und Grund der Einrichtung und Befristungen.

Bei all diesen Aufzeichnungen ist auf Aktualität und Vollständigkeit zu achten.

9.2.3 Organisatorische Regelungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen

Es sind Vorkehrungen zu treffen, die in Notfällen bei Abwesenheit von MitarbeiterInnen (z. B. im Urlaubs- oder Krankheitsfall) ihren Vertretungen Zugriff auf das IT-System bzw. die Daten ermöglichen.

Generell sollte in Applikationen und IT-Systemen eine Stellvertreterregelung schon eingebaut sein, damit keine Weitergabe von Passwörtern in Abwesenheitsfällen benötigt wird.

Ist es in Einzelfällen doch notwendig, ein Passwort zu hinterlegen, so ist dieses an einem geeigneten, geschützten Ort (z. B. in einem Tresor) zu deponieren und bei jeder Änderung des Passwortes zu aktualisieren (regelmäßige Prüfung auf Aktualität erforderlich!). Wird es notwendig, dieses hinterlegte Passwort zu nutzen, so sollte dies nach dem Vier-Augen-Prinzip, d. h. von zwei Personen gleichzeitig, geschehen.

Ist vom System technisch kein Vier-Augen-Prinzip vorgesehen, so lässt sich dieses auch organisatorisch nachbilden, indem Passwörter in mehrere Teile zerlegt werden, wobei alle im Notfall Zugriffsberechtigten nur einen Teil besitzen.

Nach der Rückkehr der BenutzerInnen sind diese über die Weitergabe des Passworts in Kenntnis zu setzen und es ist ein neues Passwort von ihnen zu vergeben. Außerdem ist die Weitergabe des Passworts und deren Dauer zu dokumentieren.

Je nach den technischen Möglichkeiten können auch „Einmalpasswörter“ oder Passwörter mit begrenzter Benutzungsdauer vergeben werden.

Beim Einsatz von Chipkarten zur Authentisierung sind Vorkehrungen zu treffen, die es erlauben, bei momentaner Inoperabilität bzw. Nichtverfügbarkeit der Chipkarte Berechtigten den Zugang zum System zu ermöglichen. Abhängig von den Personalisierungsmöglichkeiten vor Ort ist dafür Sorge zu tragen, dass eine zeitgerechte Neuausstellung der Karte oder eine Ausstellung einer temporär gültigen Karte möglich ist oder aber Ersatzkarten zur Verfügung stehen.

9.3 Verantwortung der BenutzerInnen

Die BenutzerInnen sind verantwortlich, die Mechanismen gegen unbefugten Zugriff, Kompromittierung oder Diebstahl von Informationen bzw. Einrichtungen wirksam zu halten. Allerdings sind sie diesbezüglich mit verständlichen Anweisungen zu unterstützen.

9.3.1 Regelungen des Passwortgebrauches

Erfolgt die Authentisierung in einem IT-System über Passwörter, so ist die Sicherheit der Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gewählt und verwendet wird. Dafür ist es empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen, die BenutzerInnen diesbezüglich zu unterweisen und die Einhaltung zu kontrollieren.

Regelungen zum Passwortgebrauch sind in hohem Maße abhängig vom betroffenen IT-System, dem Schutzbedarf der darauf laufenden Anwendungen bzw. der gespeicherten Daten sowie den auf dem System realisierten technischen Möglichkeiten.

Im Folgenden werden jedoch einige Grundregeln gegeben, die eine Art **Mindeststandard für die Wahl und die Handhabung von Passwörtern** darstellen. Für BenutzerInnen mit umfangreichen Rechten, wie etwa AdministratorInnen, bzw. in Bereichen, in denen mit streng vertraulichen Informationen gearbeitet wird, werden die Anforderungen i. Allg. höher liegen.

- Das Passwort muss so komplex sein, dass es nicht leicht zu erraten ist. Es sollte jedoch auch nicht zu kompliziert sein, damit es für BenutzerInnen noch leicht merkbar ist und sie in der Lage sind es regelmäßig zu verwenden.
- Die Komplexität eines Passworts (z.B. Verwendung von Groß- und Kleinbuchstaben, Ziffern oder Sonderzeichen) steht im Verhältnis zu dessen Länge. Bei einem längeren Passwort kann auf etwas Komplexität verzichtet werden, ein sehr komplexes Passwort kann kürzer sein, wobei jedoch eine Mindestlänge von 8 Zeichen nicht unterschritten werden sollte.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl), idealerweise jedoch mindestens ein Zeichen aus drei der vier Kategorien (Groß-, Kleinbuchstaben, Ziffern oder Sonderzeichen).
- In Verbindung mit weiteren Authentifizierungsfaktoren können sich auch geringere Anforderungen ergeben.
- Die Mindestlänge eines Passworts hängt auch immer vom konkreten Anwendungsfall ab. Je sicherheitsrelevanter der geschützte Zugang ist, desto stärker und somit auch länger sollte das zugehörige Passwort sein. Behördliche Zugänge etwa, sollten auch trotz komplexer Passwörter nicht nur auf 8 Zeichen vertrauen und außerdem sofern möglich mindestens einen weiteren Faktor erfordern. Ein Anwendungsgebiet in dem Offline-Attacken auf den Passwort-Hash möglich sind, wie z.B. für WLAN-Zugänge, erfordert um einiges längere Passwörter, beispielsweise ab 20 Zeichen, oder einen regelmäßigen Passwortwechsel.
- Wörter die in einem Wörterbuch, egal welcher Sprache, vorkommen dürfen nie als alleiniges Passwort dienen, sie können aber ein Teil des Passworts sein. In diesem Fall sollten sie jedoch als einzelnes Zeichen betrachtet werden. Das sehr schlechte Passwort „mein_Zugang“ wäre nach dieser Betrachtungsweise somit 3 Zeichen lang. Um diese Einschränkung zu umgehen, können die einzelnen Wörter auch geteilt und mit Ziffern oder Sonderzeichen ersetzt oder verbunden sowie Groß- und Kleinschreibung geändert werden. Ein mögliches Resultat wäre beispielsweise „me#z08än8#IN“.
- Passwörter mit spezieller, von Außenstehenden leicht zu erratender Bedeutung, wie Namen, Geburtsdaten, Firmen- oder Abteilungsbezeichnungen, Kfz-Kennzeichen etc. sind ebenso zu vermeiden wie Standardausdrücke wie TEST, SYSTEM und Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456 etc.
- Sofern anwendbar, sollte der Einsatz eines Passwort-Managers zur Generierung und Verwaltung der Passwörter evaluiert werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen umgehend durch individuelle Passwörter ersetzt werden. Der Hersteller bzw. Lieferant sollte dazu nach allen voreingestellten Benutzerkennungen und Passwörtern befragt werden.
- Es ist zu prüfen, ob das Berechtigungssystem alle Stellen des Passwortes oder nur Teile davon überprüft.

- Dasselbe Passwort darf nicht für verschiedene Dienste bzw. Konten verwendet werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.
- Bei der Eingabe darf das Passwort nicht auf dem Bildschirm angezeigt werden.
- Das Passwort muss geheim gehalten werden und sollte nur den jeweiligen BenutzerInnen persönlich bekannt sein.
- Das Passwort sollte nach Möglichkeit nicht schriftlich fixiert werden. Wird es doch aufgeschrieben, so ist für die Sicherheit dieser Aufzeichnungen besonders Sorge zu tragen.
- Ist das Passwort unautorisierten Personen bekannt geworden, so ist ein sofortiger Passwortwechsel durchzuführen.

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern (s. o.) sollte mit technischen Mitteln verhindert werden („Stoppwortliste“).
- Alle BenutzerInnen müssen ihr eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer BenutzerInnen sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.
- Nach einer vorgegebenen Anzahl von Fehlversuchen (meist 3) ist eine vordefinierte Aktion zu setzen. Eine solche Aktion kann etwa eine Sperre der Benutzer-ID sein, die nur von SystemadministratorInnen aufgehoben werden kann, aber auch eine Sperre des Gerätes oder ein Timeout, eine Warnmeldung oder Ähnliches.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter bzw. deren Hash verschlüsselt übertragen werden.
- Die Passwörter sollten im System zugriffssicher und nicht im Klartext gespeichert werden, z. B. mittels Einwegverschlüsselung.
- Sofern es nicht möglich ist eine Kompromittierung von Passwörtern zu erkennen, können auch zeitgesteuerte Passwortwechsel angewendet werden. Dabei sollten jedoch die dadurch möglicherweise auftretenden Nachteile (z.B. Verwendung von weniger komplexen Passwörtern, Passwörter werden eher notiert, Passwörter werden eher vergessen wodurch auf Konten oder Ressourcen nicht mehr zugegriffen werden kann) bedacht werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden. Dazu sollten die Hashwerte aller alten Passwörter bzw. eine größere Anzahl zum Vergleich herangezogen werden (Passwort-Historie).
- Ebenso sollte das Setzen bereits kompromittierter Passwörter unterbunden werden, indem diesbezügliche öffentliche Datenbanken abgefragt werden.

Als weitere Hilfestellung sei hierzu auf die Checkliste „Sichere Passwörter“ verwiesen. Diese enthält Kriterien für die sichere Passwortauswahl und -verwendung sowie weiteren optionalen Maßnahmen. Je nach Organisationsvorgaben oder Anwendungsbereich kann sie direkt herangezogen werden oder aber als Vorlage und Denkanstoß für spezifischere Bereiche dienen.

Für Behörden und Unternehmen eignen sich außerdem die Anforderungen aus dem IT-Grundschutz-Baustein ORP.4 Identitäts- und Berechtigungsmanagement des BSI. Tiefgreifendere und technischere Vorgaben liefert die NIST Special Publication 800-63B.

9.3.2 Bildschirmsperre

Unter einer Bildschirmsperre versteht man die Möglichkeit, die auf dem Bildschirm aktuell vorhandenen Informationen zu verbergen. Die Aktivierung der Bildschirmsperre sollte erfolgen, wenn die BenutzerInnen den Arbeitsplatz für eine kurze Zeit verlassen.

Als weiteres Leistungsmerkmal sollte die Bildschirmsperre eine automatische Aktivierung bei längerer Pausenzeit aufweisen. Verfügt das Softwareprodukt außerdem über eine Passwortabfrage, wird bei Abwesenheit der BenutzerInnen zusätzlich ein Zugriffsschutz für das IT-System gewährleistet.

Beim Einsatz von Chipkarten soll gewährleistet sein, dass die Bildschirmsperre nur mittels Chipkarte und PIN wieder aufgehoben werden kann. Beim Entfernen der Chipkarte ist entweder die Bildschirmsperre zu aktivieren oder die BenutzerInnen sind auszuloggen.

9.4 Fernzugriff

Neben der Sicherheit von Serversystemen und Endgeräten wird die eigentliche Netzinfrastruktur mit den aktiven Netzkomponenten in vielen Fällen vernachlässigt. Gerade zentrale aktive Netzkomponenten müssen jedoch sorgfältig konfiguriert werden. Denn während durch eine fehlerhafte Konfiguration eines Serversystems nur diejenigen BenutzerInnen betroffen sind, die die entsprechenden Dienste dieses Systems nutzen, können bei einer Fehlkonfiguration einer Netzwerkkomponente größere Teilnetze bzw. sogar das gesamte Netz ausfallen oder Daten unbemerkt kompromittiert werden.

Für aktive Netzkomponenten mit Routing-Funktionalität ist außerdem ein geeigneter Schutz der Routing-Updates erforderlich. Diese sind zur Aktualisierung der Routing-Tabellen erforderlich, um eine dynamische Anpassung an die aktuellen Gegebenheiten des lokalen Netzes zu erreichen. Ein solcher Schutz ist zum einen durch Passwörter, zum anderen durch kryptographische Prüfsummen erreichbar.

Behörden und Unternehmen müssen häufig Fernzugriffsmöglichkeiten auf ihre IT-Systeme einrichten, um auf Daten und Anwendungen unabhängig vom Standort dieser Institution zugreifen zu können.

Diese Fernzugriffsmöglichkeiten können mit unterschiedlichen Endgeräten (Desktop, Notebook, Smartphone, …) realisiert werden. Die Verbindung zwischen dem Endgerät und der Zentrale führt in der Regel über das Internet, auf das wiederum über Kabel-Anschlussleitungen, 5G, WLAN oder öffentliche Telefonnetze etc. zugegriffen werden kann.

Mit dem Gewinn an Flexibilität sind Risiken verbunden, die vor allen Dingen die Möglichkeit der Spionage und des Verlusts von Daten sowie der Sabotage der IT-Systeme der Institution betreffen.

Zu den wichtigsten Maßnahmen gehören

- eine erfolgreiche Authentifizierung der BenutzerInnen gegenüber ihren Endgeräten und dem Netz der Institution,
- Verschlüsselung der Daten auf dem Endgerät und eine regelmäßige Sicherung der Daten im Netz der Institution, um die auf dem Endgerät gespeicherten Daten vor Verlust und gegen Vertraulichkeitsverletzungen zu schützen
- Einsatz eines kryptografisch gesicherten VPN, um die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution vor unbefugtem Mitlesen zu schützen.

Wurden Endgeräte entwendet oder gestohlen, sollten sich die Fernzugriffe der betroffenen BenutzerInnen durch die Institution kurzfristig sperren lassen. Zusätzlich sollte eine Anwenderrichtlinie die BenutzerInnen auf ihre Sorgfaltspflichten hinweisen, um so die Risiken durch Nachlässigkeit zu reduzieren.

9.4.1 Nutzung eines Authentisierungsservers beim Fernzugriff

Für Netzwerke mit vielen BenutzerInnen sollte auf die Effizienz der Benutzerverwaltung auch für Fernzugriffe geachtet werden.

Für mittlere und große Netze, die organisatorisch meist in mehrere Teilnetze (Domänen, Verwaltungsbereiche) aufgeteilt sind, besteht in vielen Fällen das Problem, dass in jedem Verwaltungsbereich eine getrennte Verwaltung der Benutzerdaten durchgeführt wird. Sollen sich BenutzerInnen auch an fremden Teilnetzen anmelden können, müssen hier Querberechtigungen (Cross-Zertifikate, Vertrauensstellungen) oder ein zentraler Verzeichnisdienst eingerichtet und gepflegt werden.

Insbesondere im Kontext mit Fernzugriffen haben sich hier spezielle Authentisierungssysteme herausgebildet, die auch für den „normalen“ Authentisierungsprozess bei der Systemanmeldung genutzt werden können.

Prinzipiell besitzen diese Systeme folgenden Aufbau:

- Die Authentisierungsdaten der BenutzerInnen werden durch einen zentralen Server verwaltet.
- Das Programm zur Systemanmeldung wendet sich zur Überprüfung der von den BenutzerInnen eingegebenen Authentisierungsdaten an den Authentisierungsserver.
- Zur Kommunikation zwischen Anmeldeprozess und Authentisierungsserver wird in der Regel ein abgesichertes Protokoll eingesetzt.

Der Anmeldeprozess muss dazu die Nutzung externer Authentisierungsserver unterstützen und die Netzadresse des zu benutzenden Authentisierungsservers muss in den Konfigurationsdaten des Anmeldeprozesses korrekt eingetragen sein. Wollen sich BenutzerInnen nun am System anmelden - gleichgültig ob sie dazu eine RAS-Verbindung benutzen oder sich direkt im LAN befinden - laufen grob vereinfacht folgende Schritte ab:

- Findet ein Verbindungsaufbau mit dem Anmeldeprozess statt, kontaktiert dieser den Authentisierungsserver und informiert ihn über den eingegangenen Verbindungswunsch von BenutzerInnen. Der Authentisierungsserver sendet - sofern ein „Challenge-Response“ Verfahren zum Einsatz kommt - eine so genannte „Challenge“ an den Prozess zurück, der diese an die jeweiligen BenutzerInnen weiterleitet.
- Die BenutzerInnen geben ihr jeweiliges Authentisierungsgeheimnis ein. Dies kann je nach verwendetem System ein Passwort oder ein Einmalpasswort in den unterschiedlichsten Ausprägungen (Nummern, Text) sein.
- Der Anmeldeprozess leitet die Daten (meist transparent für die BenutzerInnen) an den Authentisierungsserver weiter.
- Der Authentisierungsserver verifiziert die Benutzerdaten und signalisiert dem Anmeldeprozess das Ergebnis der Überprüfung.
- Der Zugang zum (Access-)Netz wird nach erfolgreicher Überprüfung gewährt.

Durch die Verwendung von zentralen Authentisierungsservern kann erreicht werden, dass einerseits die Authentisierungsdaten konsistent verwaltet werden und andererseits bessere Authentisierungsmechanismen genutzt werden können, als sie von den Betriebssystemen standardmäßig unterstützt werden. Hier sind insbesondere Mechanismen zu nennen, die auf Chipkarten oder Token basieren. Je nach System erzeugen diese z. B. Einmalpasswörter, die auf einem Display angezeigt werden und welche die BenutzerInnen als Passwort angeben müssen.

Für mittlere und große Netze wird die Verwendung von Authentisierungsservern insbesondere bei Fernzugriffen empfohlen, da diese eine wesentlich höhere Sicherheit bei der Benutzerauthentisierung bieten. Berücksichtigt werden muss jedoch, dass auch diese Server administriert und gewartet werden müssen. Ein Authentisierungsserver muss so im Netz platziert werden, dass er einerseits performant erreicht werden kann, aber andererseits auch vor unberechtigten Zugriffen geschützt ist.

9.4.2 Einsatz geeigneter Tunnelprotokolle für die VPN-Kommunikation

Wird über ein Virtual Private Network (VPN) auf ein LAN zugegriffen, so erfolgt der Zugriff typischerweise über eine externe Datenverbindung. So wird beispielsweise bei einer direkten Einwahl das Netz eines Telekommunikationsanbieters benutzt. Wird die Verbindung über das Internet aufgebaut, werden die Daten über die Netze der beteiligten Internetdienstanbieter (und eventuell deren Kooperationspartner) geleitet. Da über eine VPN-Verbindung die direkte Anbindung an ein LAN erfolgt, muss der zur Datenübertragung benutzte Netzpfad so abgesichert werden, dass die Vertraulichkeit, Integrität und Authentizität gewährleistet ist.

Die Absicherung wird durch das Verschlüsseln und gegebenenfalls Signieren der ausgetauschten Datenpakete erreicht, nachdem die Kommunikationspartner authentisiert wurden. Im VPN-Umfeld haben sich verschiedene Verfahren und Mechanismen zur Absicherung der Kommunikationsverbindung herausgebildet, wie beispielsweise das Tunneling (vgl. 13.1.10 Remote Access).

Die Wahl des Verfahrens, das zur Absicherung einer VPN-Verbindung zu benutzen ist, hängt von verschiedenen Faktoren ab, u.A.

- von den Sicherheitsanforderungen an die Stärke der Verfahren (hierdurch werden beispielsweise die Schlüssellängen bestimmt),
- von den auf Protokollebene einsetzbaren Verfahren (siehe unten),
- von den durch die VPN-Hard- und Software unterstützten Verfahren.

Generell gilt:

- Ein VPN-Produkt bietet in der Regel eine Auswahl von unterstützten Standardverfahren zur Kommunikationsabsicherung an. Hier sollte eine möglichst breite Unterstützung von Verfahren angestrebt und entsprechende Standards angewendet werden (beispielsweise IPsec oder TLS).
- Die zum Datentransport benutzten Protokolle bieten selbst schon Sicherheitsmechanismen an. Diese können vom VPN-Produkt genutzt werden. Alternativ kann das VPN-Produkt auch eigene Verfahren anbieten.

Die Sicherheitsmechanismen basieren auf unterschiedlichen kryptographischen Verfahren.

9.4.3 Einsatz von Modems

Modems werden angesichts der besseren Möglichkeiten durch Breitband-Internet bzw. Mobilfunk immer seltener verwendet. Einige der hier angeführten Grundsätze gelten allerdings auch für solche, und es gibt nach wie vor noch Modemzugänge. Für den sicheren Einsatz sind eine Reihe von Regelungen zu treffen.

So ist etwa festzulegen

- wer die Verantwortlichen für den sicheren Betrieb der Modems sind (beispielsweise im Stand-alone Einsatz die IT-BenutzerInnen, in vernetzten Systemen die AdministratorInnen),
- wer das Modem benutzen darf,
- in welchen Fällen vertrauliche Informationen bei der Übertragung verschlüsselt werden müssen,
- in welchen Fällen durchgeführte Datenübertragungen zu protokollieren sind (z. B. bei Übermittlung personenbezogener Daten). Bietet die Kommunikationssoftware Protokollierungsfunktion an, sollten diese im sinnvollen Rahmen genutzt werden.

Alle Login-Vorgänge, ob erfolgreich oder erfolglos, müssen protokolliert werden. Korrekt eingegebene Passwörter sollten nicht mitprotokolliert werden, es ist aber zu überlegen, die bei erfolglosen Login-Versuchen eingegebenen Passwörter mitzuprotokollieren, um Passwortattacken zu entdecken.

Der sichere Einsatz eines Modems bedingt weiters einige administrative Maßnahmen:

- Die Telefonnummer eines Modemzugangs darf nur den KommunikationspartnerInnen bekannt gegeben werden, um den Zugang vor Einwählversuchen zu schützen. Sie darf nicht im Telefonverzeichnis der Organisation erscheinen.
- Ist ein Modem in einen Netzserver integriert, können BenutzerInnen von ihren Arbeitsplatzrechnern auf das Modem zugreifen. Dann darf ein Zugriff auf die Kommunikationssoftware nur den BenutzerInnen möglich sein, die für die Datenübertragung berechtigt sind.
- Außerdem müssen regelmäßig die Einstellungen des Modems und der Kommunikationssoftware überprüft werden sowie die durchgeführten Datenübertragungen protokolliert werden.

- Es muss sichergestellt sein, dass das Modem die Telefonverbindung unterbricht, sobald sich die Benutzerin/der Benutzer vom System abmeldet. Bei einem Stand-alone-System kann dies dadurch realisiert sein, dass das Modem nur solange mit dem Telefonnetz verbunden ist, wie es für die Datenübertragung eingesetzt wird, und es anschließend ausgeschaltet bzw. von der Leitung getrennt wird. Bei einem im Netzserver integrierten Modem muss dies über die Konfiguration sichergestellt werden. Ein externes Modem kann einfach ausgeschaltet werden. Außerdem müssen alle BenutzerInnen darauf hingewiesen werden, dass nach der Datenübertragung auch das Kommunikationsprogramm zu beenden ist.
- Es muss außerdem darauf geachtet werden, dass nach einem Zusammenbruch der Modemverbindung externe BenutzerInnen automatisch vom IT-System ausgeloggt werden. Andernfalls kann die nächste Anruferin/der nächste Anrufer eventuell unter dieser Benutzerkennung weiterarbeiten, ohne sich anzumelden.

Sicherheitsmechanismen bei Modems

Es gibt vielfältige Sicherheitsmechanismen, die in Modems integriert sein können, wie etwa Passwortmechanismen oder Callback-Funktionen (vgl. dazu 9.4.4 Geeignete Modemkonfiguration). Einige Modems bieten auch die Möglichkeit, die übertragenen Daten zu verschlüsseln.

Die Anschaffung eines Modems mit Verschlüsselungsoption ist vorteilhaft, wenn regelmäßig Übertragungen großer Datenmengen innerhalb einer Organisation mit verstreuten Liegenschaften durchgeführt werden sollen. Diese Online-Verschlüsselung bedingt einen geringeren organisatorischen Aufwand als das Verschlüsseln der Daten mittels Zusatzprodukten. Es ist darauf zu achten, dass die eingesetzten Algorithmen stets dem Stand der Technik entsprechen.

Die vielfach angebotene Callback-Funktion bietet unter Sicherheitsgesichtspunkten den Vorteil, dass auf einfache Weise unautorisierte AnruferInnen abgewiesen werden können (siehe auch 9.4.5 Aktivierung einer vorhandenen Callback-Option).

9.4.4 Geeignete Modemkonfiguration

Die meisten Modems arbeiten nach dem nicht normierten, herstellerabhängigen Hayes-Standard (auch AT-Standard genannt). Die Basisbefehlssätze der verschiedenen Modems stimmen größtenteils überein, größere Abweichungen gibt es in den erweiterten Befehlssätzen. Es ist wichtig, den Befehlssatz des eingesetzten Modems daraufhin zu überprüfen, wie die im folgenden beschriebenen Funktionen umgesetzt sind und ob durch fehlerhafte Konfiguration Sicherheitslücken entstehen können.

Die gewählten Einstellungen sollten im nichtflüchtigen Speicher des Modems gespeichert werden. Außerdem sollten sie auf Papier ausgedruckt werden, so dass sie jederzeit mit der aktuellen Einstellung verglichen werden können.

Nachfolgend werden einige sicherheitsrelevante Konfigurationen vorgestellt:

- Auto-Answer
  Es kann eingestellt werden, dass das Modem einen ankommenden Ruf automatisch nach einer einzustellenden Anzahl von Klingelzeichen entgegennimmt. Eine Einstellung, die dies verhindert und erzwingt, dass Anrufe manuell entgegengenommen werden müssen, sollte gewählt werden, wenn verhindert werden soll, dass von außen unbemerkt eine Verbindung aufgebaut werden kann. Ansonsten ist ein Callback-Mechanismus einzusetzen (siehe 9.4.5 Aktivierung einer vorhandenen Callback-Option).
- Fernkonfiguration des Modems
  Manche Modems können so eingestellt werden, dass sie von entfernten Modems fernkonfiguriert werden können. Es ist darauf zu achten, dass diese Möglichkeit ausgeschaltet ist. Zum Problem der Fernwartung über Modems siehe 14.6.3 Fernwartung.
- Passwortgeschützte Speicherung von (Rückruf-)Nummern
  Bei der Speicherung von Telefonnummern oder Rückrufnummern im nichtflüchtigen Speicher des Modems können diese bei vielen Modellen durch ein Passwort geschützt werden. Wenn diese Möglichkeit vorhanden ist, sollte sie genutzt und die Passwörter entsprechend den Sicherheitsanforderungen (vgl. dazu auch 9.3.1 Regelungen des Passwortgebrauches) gewählt werden. Bei einigen Modems wird nach Eingabe eines bestimmten Befehls eine Liste der Rufnummern mit den zugehörigen Passwörtern angezeigt. Daher sollte der Zugang zum Modem nur befugten Personen möglich sein.

9.4.5 Aktivierung einer vorhandenen Callback-Option

Viele Modems bieten die Option eines automatischen Rückrufs (Callback). Ist diese Option aktiviert, trennt das Modem, wenn es einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Leitung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Modemzugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn feste KommunikationspartnerInnen sich automatisch einwählen können sollen. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Anmerkung: Privilegierte BenutzerInnen können evtl. die Möglichkeit haben, die Nummer einzugeben, unter der sie sich zurückrufen lassen möchten. Hier sollte darauf geachtet werden, dass nur in der Zentrale festgelegte Nummern zurückgerufen werden, und kein „Overrulen“ durch den Anrufer möglich ist.

Es ist darauf zu achten, dass der automatische Rückruf nur auf einer Seite aktiviert ist, da der Mechanismus sonst in eine Endlosschleife führt. Callback sollte auf der passiven Seite aktiviert sein, also auf der Seite, von der Dateien abgerufen oder auf der Dateien eingespielt werden.

Es ist sicherzustellen, dass die voreingestellten Rufnummern des Callbacks sporadisch kontrolliert und aktualisiert werden.

Ein Callback kann außer durch das Modem auch von der Applikation ausgelöst werden. Wenn die eingesetzte Applikation diese Option bietet, sollte das Callback von der Applikation und nicht vom Modem ausgelöst werden. Wenn das Modem ein Callback auslöst, kann ein Angreifer versuchen, in dem Moment, wenn das Modem den Callback starten will, dieses anzuwählen und damit den Callback abzufangen. Wenn die Applikation den Callback durchführt, ist es für einen Angreifer wesentlich schwieriger, den richtigen Moment abzupassen.

9.5 Zugriff auf Betriebssysteme

Die Hauptaufgabe eines Betriebssystems besteht bis heute darin, BenutzerInnen und Anwendungen den komfortablen Zugang zur Hardware und anderen Betriebsmitteln des Computersystems zu ermöglichen. Neben diesen Grundfunktionen muss ein Betriebssystem grundlegende Sicherheitskonzepte durchsetzen. Dazu gehört insbesondere sowohl der Schutz der Betriebssystemsoftware selbst als auch der Schutz einzelner Daten und Programme vor unberechtigter Benutzung (Verletzung der Vertraulichkeit von Informationen), Verfälschung (Verletzung der Integrität von Daten), vorübergehender oder dauerhafter Unbrauchbarmachung und Zerstörung (Verletzung der Verfügbarkeit von Informationen und Programmen).

9.5.1 Sichere Initialkonfiguration und Zertifikatsgrundeinstellung

Bei Neuinstallationen von Betriebssystemen und Software berücksichtigen die standardmäßigen und herstellerseitigen Grundeinstellungen kaum sicherheitstechnische Aspekte. Somit werden im Zuge von Standardkonfigurationen zur Verfügung stehende Sicherheitsmechanismen oft nicht aktiviert, bzw. bieten grundsätzliche Fehlkonfigurationen potenzielle Sicherheitsrisiken.

Um dem entgegenzuwirken ist die Verwendung von geprüften Initialkonfigurationen zu bevorzugen. Derartige Konfigurationen sollten sowohl für das Betriebssystem (vorrangig) aber auch für die verwendete Software von der Administration zur Verfügung gestellt werden.

Im Bundesbereich ist gemäß dem IKT-Board-Beschluss [IKTB-170902-7] eine definierte sichere Initialkonfiguration zu verwenden. Eine entsprechend dokumentierte Initialkonfiguration wird im Rahmen des Online-Angebotes des Chief Information Office des Bundes zur Verfügung stehen.

Zertifikatsgrundeinstellung

Voreingestellt in Betriebssystemen bzw. in Internetprogrammen (zum Beispiel Browsern) ist eine Vielzahl von „vertrauenswürdigen“ Zertifizierungsstellen, deren Zertifikaten dadurch explizit vertraut wird. Dies stellt ein Sicherheitsrisiko dar, denn die AnwenderInnen haben in der Regel keine Informationen über die Vertrauenswürdigkeit der Zertifizierungsstellen bzw. ob deren Zertifikate zwischenzeitlich bereits kompromittiert wurden. Demnach sollten in der Initialkonfiguration alle im Zertifikatsspeicher vorkonfigurierten Wurzelzertifikate (vertrauenswürdige Stammzertifikate) entfernt bzw. durch einen definierten Satz an als vertrauenswürdig anerkannten Zertifikaten ersetzt werden.

Nach IKT-Board-Beschluss [IKTB-040402-2] sind alle in der Bundesverwaltung auszuliefernden Arbeitsstationen initial so auszuliefern, dass keinem Zertifizierungsdienst automatisch vertraut wird. Das implizite Vertrauen kann allen Zertifizierungsdiensten und den zugeordneten Diensten, die der EU Signaturrichtlinie (Art. 5.1) genügen, explizit ausgesprochen werden, wenn in den Arbeitsstationen die Mechanismen des Widerrufs hinreichend umgesetzt sind. Anderen Zertifizierungsdiensten kann im bereichs-/ressortübergreifenden Datenverkehr nur dann das Vertrauen im System implizit gegeben werden, wenn dies in der allgemeinen Strategie explizit festgehalten ist.

9.5.2 Nutzung der BIOS-Sicherheitsmechanismen

Moderne BIOS-Varianten, wie zum Beispiel UEFI (Unified Extensible Firmware Interface), bieten eine Vielzahl von Sicherheitsmechanismen an, mit denen sich die BenutzerInnen oder die Systemadministration vertraut machen sollten. Auf keinen Fall sollten aber ungeschulte BenutzerInnen BIOS-Einträge verändern, da hierdurch schwerwiegende Schäden verursacht werden können.

- Schreibschutz:

Viele Mainboards besitzen einen Hardware-Schreibschutz für das BIOS (meist in Form eines Jumpers auf dem Mainboards). Sofern ein solcher Schreibschutz existiert, sollte er genutzt werden und nur bei notwendigen BIOS-Änderungen entfernt werden, z. B. nach einem nötigen BIOS-Update. Anschließend sollte er wieder gesetzt werden.

- Passwortschutz:
  Bei den meisten BIOS-Varianten kann ein Passwortschutz aktiviert werden. Dieser ist teilweise verhältnismäßig einfach überwindbar, sollte aber auf jeden Fall benutzt werden, wenn keine anderen Zugriffsschutzmechanismen zur Verfügung stehen. Meist kann ausgewählt werden, ob das Passwort vor jedem Rechnerstart oder nur vor Zugriffen auf die BIOS-Einstellungen überprüft werden soll. Teilweise können sogar verschiedene Passwörter für diese Prüfungen benutzt werden. Um zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern, sollte das Setup- oder Administrator-Passwort immer aktiviert werden. Mit einigen (leider wenigen) BIOS-Varianten kann zusätzlich der Zugriff auf USB-Ports durch ein Passwort geschützt werden. Dies sollte benutzt werden, um das unbefugte Einspielen von Software oder das unbemerkte Kopieren von Daten zu verhindern.
- Boot-Reihenfolge:
  Die Boot-Reihenfolge sollte so eingestellt sein, dass immer als Erstes von der Festplatte gebootet wird. Beispielsweise sollte also _C,E_ bzw. _C,E,A_ eingestellt werden (Annahme, dass es ein DVD-Laufwerk E gibt). Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich eine DVD im Laufwerksschacht vergessen wird, spart Zeit und schont das DVD-Laufwerk. Je nach verwendetem BIOS und Betriebssystem muss auch das Booten von anderen austauschbaren Datenträgern wie USB-Ports verhindert werden. Ohne eine solche Umstellung der Boot-Reihenfolge können auch weitere Sicherheitsmaßnahmen wie etwa Zugriffsschutzmechanismen umgangen werden. Ein Beispiel hierfür ist das Starten eines anderen Betriebssystems, so dass gesetzte Sicherheitsattribute ignoriert werden. Generell sollte die Wirksamkeit der Umstellung der Boot-Reihenfolge durch einen Boot-Versuch geprüft werden, da einige Controller die interne Reihenfolge außer Betrieb nehmen und eine getrennte Einstellung erfordern.
- Virenschutz, Virus-Warnfunktion:
  Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Bootsektors bzw. des MBR (Master Boot Record) eine Bestätigung, ob diese durchgeführt werden darf. Wird die Virus-Warnfunktion von der BIOS-Version unterstützt, sollte diese Funktion als zusätzlicher Schutz aktiviert werden.

9.6 Zugriff auf Anwendungen und Informationen

Grundsätzlich sollten MitarbeiterInnen natürlich sorgfältig mit allen Informationen umgehen. Darüber hinaus gibt es aber in vielen Bereichen Daten, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten. Für diese gelten je nach ihrer Kategorisierung unterschiedliche Beschränkungen im Umgang mit ihnen. Daher ist es wichtig, alle Mitarbeiter auf die für diese Daten geltenden Restriktionen hinzuweisen.

Der Schutzbedarf von Daten wirkt sich natürlich unmittelbar auf alle Medien aus, auf denen diese gespeichert oder verarbeitet werden. Daten mit besonderem Schutzbedarf können in den unterschiedlichsten Bereichen anfallen, z. B. bei E-Mail, daher sollten in allen diesen Bereichen Festlegungen existieren, wer solche Daten lesen, bearbeiten bzw. weitergeben darf. Dazu gehört auch die regelmäßige Überprüfung auf Korrektheit und Vollständigkeit der Daten.

Viele Informationen, aber auch Anwendungen, unterliegen Copyright-Vermerken oder Weitergaberestriktionen („Nur für den internen Gebrauch“). Alle MitarbeiterInnen müssen darauf hingewiesen werden, dass weder Dokumente, noch Dateien oder Software ohne Berücksichtigung evtl. Copyright-Vermerke oder Lizenzbedingungen kopiert werden dürfen.

Ein besonderes Augenmerk muss auch auf alle Informationen gelegt werden, welche die Grundlage für die Aufgabenerfüllung bilden. Dazu gehören alle geschäftsrelevanten Daten, also z. B. diejenigen Daten, bei deren Verlust die Organisation handlungsunfähig wird, die die Beziehungen zusammenarbeitender Organisationen beeinträchtigen können oder aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann. Jede Organisation sollte eine Übersicht darüber haben, welche Daten als geschäftskritisch einzustufen sind. Neben den allgemeinen Sorgfaltspflichten können auch hier für diese Daten bei der Speicherung, Verarbeitung, Weitergabe und Vernichtung besondere Vorschriften und Regelungen gelten.

- Geschäftskritische Informationen müssen vor Verlust, Manipulation und Verfälschung geschützt werden.
- Längerfristig gespeicherte oder archivierte Daten müssen regelmäßig auf ihre Lesbarkeit getestet werden.
- Nicht mehr benötigte Informationen müssen zuverlässig gelöscht werden.

[Quelle: BSI M 2.2.17]

9.6.1 Wahl geeigneter Mittel zur Authentisierung

Während unter „Identifikation“ die Bestimmung der Identität eines Subjektes bzw. Objektes zu verstehen ist (meist durch Angabe eines Namens oder einer User-ID), versteht man unter „Authentisierung“ den Nachweis der angegebenen Identität.

Die Wahl eines geeigneten Authentisierungsverfahrens ist von entscheidender Bedeutung für die Sicherheit des Gesamtsystems und muss daher den Sicherheitsanforderungen und den technischen Möglichkeiten gemäß getroffen werden.

Grundsätzlich gibt es drei Arten der Authentisierung:

- Authentisierung durch Wissen: etwa durch Eingabe von Passwörtern, Codes, kryptographischen Schlüsseln
- Authentisierung durch Besitz: beispielsweise von Schlüsseln oder Karten
- Authentisierung durch Eigenschaften oder Verhaltensmerkmale (biometrische Verfahren): z. B. Unterschriftendynamik, Stimmerkennung, Fingerabdruck, …

Die Sicherheit der einzelnen Authentisierungsverfahren ist sehr unterschiedlich und im Einzelfall immer zu hinterfragen. In vielen Fällen kommen Multifaktorauthentisierungen (Kombinationen der drei angeführten Prinzipien - etwa Authentisierung durch Wissen und Besitz) zur Anwendung (Mehrfaktorauthentisierung).

Im Bereich der öffentlichen Verwaltung wird die Verwendung von so genannten Dienstkarten, gemäß der Empfehlung des IKT-Boards [IKTB-140102-1] , zur Identifikation bzw. Authentisierung vorzusehen sein.

Darüber hinaus ist generell zu prüfen, ob bei Verfahren der öffentlichen Verwaltung das gemäß dem IKT-Board-Beschluss festgelegte Konzept „Bürgerkarte“ zur Authentisierung von BenutzerInnen anzuwenden ist. Weiters besteht die Möglichkeit, in Verbindung mit der Bürgerkarte so genannte Single-Sign-On-Funktionalitäten zu realisieren.

Für die Signatur und die Identifikation wird empfohlen die Module für Onlineverfahren (MOA-ID, MOA-SS/SP) zu verwenden ([IKTB-161203-01]). Diese Module stehen auch der Wirtschaft frei zur Verfügung ([IKTB-110504-1]). Gemäß dem IKT-Board-Beschluss [IKTB-260701-1] soll sogar anstelle eines konventionellen Single-Sign-On die Identifikation mit der Bürgerkarte, unter Verwendung geeigneter Basisdienste, treten.

Nach der Auswahl eines geeigneten Authentisierungsverfahrens sind Regelungen über die Handhabung der Authentifikationsmitteln zu treffen (vgl. dazu auch 9.3.1 Regelungen des Passwortgebrauches und 9.6.2 Regelungen des Gebrauchs von Chipkarten).

Biometrie

In der Diskussion um Mittel der Authentifikation rückt auch Biometrie zunehmend in den Mittelpunkt. Biometrie kann allerdings noch nicht in allen Bereichen der Identifikation und Authentifikation – im Speziellen im Sinne eines authentischen Identitätsnachweises - als technisches Mittel der Wahl angesehen werden.

Die Stabsstelle IKT-Strategie des Bundes hat im Rahmen des IKT-Board-Beschlusses [IKTB-110903-10] , insbesondere im Hinblick auf den Einsatz der Biometrie in Bereichen der öffentlichen Verwaltung, die folgenden allgemeinen Umsetzungsrichtlinien beschlossen:

- Eine hohe Funktionsstärke (Strength of Function - SOF - high vgl. Stärke der Mechanismen) ist derzeit und in absehbarer Zukunft nicht erreichbar, daher ist vorerst nur limitierter Einsatz der Biometrie möglich.
- Standards für biometrische Merkmale, die eine dauerhafte (etwa 10-jährige) Sicherheit gewährleisten, sind noch nicht vorhanden, daher können zentrale Datenbanken nicht sinnvoll eingesetzt werden.
- Die Identifikationsanwendung außerhalb der erkennungsdienstlichen Aufgaben ist noch nicht technologisch rechtfertigbar.
- Anwendungen können im Bereich der Verifikation und der Komfortsteigerung einen wesentlichen Beitrag leisten. Verifikationsanwendungen mit biometrischen Daten unter Kontrolle des Inhabers/der Inhaberin und mit amtlicher Bestätigung (Signatur) zur breiten Anwendung sind derzeit möglich und können eingesetzt werden. Dies gilt auch für Anwendungen mit Identifikationszuordnung in beschränkten Gruppen (im Normalfall etwa bis zu 100 Personen).
- Anwendungen müssen zurzeit in kontrollierter Umgebung ablaufen. Der Machtgeber für das Identifikationsobjekt (z. B. Computer, Daten etc.) muss die Möglichkeit der Kontrolle des Verifikationsprozesses haben.

Derzeit praktikable Anwendungen für Biometrie sind z. B.:

- Personendokumente mit biometrischen Daten auf dem Dokument, die durch die Behörde bestätigt (signiert) sind.
- Zuordnung von Chipkarten zu Personen (dies ist vom Willensakt der Auslösung einer Funktion zu trennen, da Wachzustand und Bewusstsein zurzeit in biometrischen Systemen nicht mit vertretbarem Aufwand technisch kontrollierbar sind).
- Zutrittskontrolle zu Anlagen und Räumen vor allem über Sekundärmechanismen (z. B. biometrisches Merkmal und Karte als Träger der Referenzdaten) oder in beschränkten Populationen.

9.6.2 Regelungen des Gebrauchs von Chipkarten

Für Anwendungen im Sicherheitsbereich kommen intelligente Speicherkarten (Karten mit fest verdrahteter Sicherheitslogik) sowie Mikroprozessor-Karten (Karten mit Speicher und CPU, evtl. auch mit Co-Prozessor) zum Einsatz.

Chipkarten haben unter Sicherheitsaspekten im Wesentlichen zwei Funktionen zu erfüllen. Sie dienen

- als Trägermedium für vertrauliche Daten z. B. Chiffrierschlüssel, Signaturschlüssel zur Generierung elektronischer Unterschriften (vgl. 10.1 Kryptographische Maßnahmen), Zugangscodes (etwa zu IT-Systemen), persönliche Daten (medizinische Daten, Prüfungsergebnisse etc.)
- als Security Modul (zur Durchführung von Sicherheitsfunktionen) z. B. zur Chiffrierung, Authentisierung, Generierung von elektronischen Signaturen, Generierung von Sessionkeys oder zur Durchführung von Transaktionen

Entscheidender Vorteil der Chipkarte gegenüber anderen Medien ist, dass die Speicherung der vertraulichen Daten und die Durchführung von sicherheitskritischen Funktionen innerhalb der Karte - also in einem geschützten Bereich - erfolgen kann. Angriffe gegen diesen geschützten Bereich erfordern einen sehr hohen technologischen Aufwand. Ist mit solchen Angriffen zu rechnen, so sind eine Reihe von kryptographischen und systemtechnischen Gegenmaßnahmen zu setzen (etwa Schlüsseldiversifizierung, Verwendung kartenspezifischer Schlüssel und geeignete Implementierung von kryptographischen Algorithmen). Für Details zur Sicherheit von Chipkarten sei auf die Literatur verwiesen - im Folgenden wird der Einsatz von Chipkarten in sicherheitsrelevanten Applikationen behandelt.

Der Zugriff auf Daten und Funktionen von Chipkarten ist heute i. Allg. durch sog. PINs (Personal Identification Number) geschützt. Denkbar ist auch eine Multifaktorauthentisierung, wo eine PIN zusammen mit biometrischen Merkmalen herangezogen wird. Dadurch kann die PIN zur leichteren Handhabe verkürzt werden.

Neben der Qualität der Karte selbst kommt auch der Wahl und der Handhabung der PIN entscheidende Bedeutung für die Sicherheit des Gesamtsystems zu. Diese sind in hohem Maße abhängig vom Schutzbedarf des betroffenen Systems und der Art der Anwendung. Im Folgenden werden einige Grundregeln gegeben, die eine Art **Mindeststandard für die Handhabung von Karten und PINs in sicherheitsrelevanten Anwendungen** (etwa Zutritts- oder Zugriffskontrolle, Signatur, …) darstellen:

- Keine unautorisierte Weitergabe der Karte: Chipkarten stellen in der Regel ein persönliches Sicherheitsmedium dar und sollten daher sicher verwahrt und keinesfalls an andere Personen weitergegeben werden. Wenn erforderlich, sind die MitarbeiterInnen in entsprechenden Verpflichtungserklärungen zur

Einhaltung dieser Regelungen zu verpflichten. Die Chipkarten sollten immer mit dem Namen der Trägerin bzw. des Trägers versehen werden. Übertragbare Chipkarten ohne Namen sollten gar nicht oder nur in sicherheitstechnisch belanglosen Bereichen eingesetzt werden.

- Die PIN muss geheim gehalten werden und darf nur den jeweiligen BenutzerInnen persönlich bekannt sein.
- Ein Aufbewahren der PIN gemeinsam mit der Karte oder gar ein Notieren der PIN auf der Karte ist unbedingt zu vermeiden.
- Die Länge der PIN hängt von Art und Schutzbedarf der Anwendung ab und liegt i. Allg. zwischen 4 und 8 Stellen. Die Wahl von Trivial-PINs ist zu vermeiden.
- Da sich Chipkarten in der Regel nach einer festgelegten Anzahl von PIN-Falscheingaben (meist 3) selbst sperren - dies stellt eines der wichtigsten Sicherheitsfeatures der Karte dar -, ist eine Möglichkeit des Entsperrens vorzusehen. Dies erfolgt durch eine von der PIN unterschiedliche (und meist deutlich längere) Geheimzahl („Supervisor PIN“, „Personal Unblocking Key“ (PUK)), die entweder den BenutzerInnen selbst oder den Sicherheitsverantwortlichen bekannt sein kann.
- PINs dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Die Eingabe der PIN sollte unbeobachtet stattfinden.
- Bei der Eingabe darf die PIN nicht auf einem Bildschirm oder Display angezeigt werden.
- Es ist zu prüfen, ob eine Übertragung der PIN zwischen Tastatur und Karte im Klartext aus Sicherheitsgründen vertretbar ist. Für Anwendungen mit hohem Sicherheitsbedarf in ungeschützten bzw. unkontrollierbaren Umgebungen sollten sog. „Secure PIN-Pads“ zum Einsatz kommen, bei denen die Übertragung der PIN technisch oder mittels kryptographischer Verfahren geschützt wird.

Zusätzlich ergibt sich bei der Wahl der einzusetzenden Chipkarte, dass speziell in Verbindung mit Anwendungen der öffentlichen Verwaltung, diese den Security Layer unterstützen (vgl. [IKTB-040901-1]).

9.6.3 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

Standardprodukte im PC-Bereich bieten oft eine Reihe von nützlichen IT-Sicherheitsfunktionen, deren Güte im Einzelnen unterschiedlich sein kann, die aber Unbefugte behindern bzw. mögliche Schäden verringern können.

Im Folgenden seien einige dieser Funktionen kurz erläutert:

- Passwortschutz bei Programmaufruf:
  Das Programm kann nur gestartet werden, wenn vorher ein Passwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.

- Zugriffsschutz zu einzelnen Dateien:
  Das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Passwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.
- Automatische Speicherung von Zwischenergebnissen:
  Das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so dass ein Stromausfall nur noch die Datenänderungen betrifft, die nach der letzten automatischen Speicherung eingetreten sind. Gegebenenfalls ist jedoch zu überprüfen, ob die zwischengespeicherten Daten nach dem regulären Programmende wieder gelöscht wurden (vgl. 14.4.1 Verifizieren der zu übertragenden Daten vor Weitergabe).
- Automatische Sicherung der Vorgängerdatei:
  Wird eine Datei gespeichert, zu der im angegebenen Pfad eine Datei gleichen Namens existiert, so wird die zweite Datei nicht gelöscht, sondern mit einer anderen Kennung versehen. Damit wird verhindert, dass versehentlich eine Datei gleichen Namens gelöscht wird.
- Verschlüsselung von Dateien:
  Das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so dass eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Chiffrierschlüssel verfügen.
- Automatisches Anzeigen von Makros in Dateien:
  Diese Funktion soll das unbeabsichtigte Ausführen von Makros verhindern und damit Schutz vor Makroviren bieten (vgl. 12.3 Schutz vor Schadprogrammen und Schadfunktionen).

Je nach eingesetzter Software und damit vorhandenen Zusatzsicherheitsfunktionen kann der Einsatz dieser Funktionen sinnvoll sein. Für mobil eingesetzte IT-Systeme bieten sich insbesondere die Nutzung des Passwortschutzes bei Programmaufruf und die automatische Speicherung an.

10 Kryptographie

10.1 Einsatz kryptographischer Maßnahmen

Bei sachgemäßem Einsatz eignen sich kryptographische Verfahren gut zur Abwehr folgender Bedrohungen:

- Vertraulichkeitsverlust: Kenntnis von Informationen durch Unbefugte,
- Integritätsverlust: Manipulation von Daten durch Unbefugte und
- Authentizitätsverlust: Manipulationen an der Urheberschaft von Informationen.

Allerdings reichen kryptographische Maßnahmen allein nicht aus, um alle Bedrohungen abzuwehren:

- Kryptographische Maßnahmen tragen nichts zur Verfügbarkeit von Daten bei (im Gegenteil – unsachgemäßer Gebrauch von Verschlüsselung kann zu Datenverlust führen; auf jeden Fall kosten kryptographische Maßnahmen Systemperformance).
- Kryptographische Maßnahmen können nichts gegen Denial-of-Service-Attacken (d. s. massenweise sinnlose Transaktionen gegen ein Zielsystem, um dieses lahm zu legen) tun. Sie können aber zur Früherkennung solcher Attacken beitragen.
- Kryptographische Maßnahmen können absichtliche oder unabsichtliche (Übertragungsfehler, Rauschen) Verfälschungen von Informationen nicht verhindern, diese jedoch nachträglich erkennbar machen.

Der Einsatz kryptographischer Maßnahmen erfordert zusätzlichen Aufwand sowie je nach Komplexität der eingesetzten Produkte unterschiedlich tiefe Kenntnisse. Daher ist es sinnvoll und notwendig, dass alle MitarbeiterInnen, die kryptographische Verfahren und Produkte einsetzen sollen, über den Nutzen, die Notwendigkeit und Eigenschaften kryptographischer Maßnahmen und Verfahren informiert und sensibilisiert werden. Das gilt erst recht für diejenigen, welche ein Kryptokonzept erstellen, Kryptoprodukte auswählen, installieren oder betreuen sollen.

Grundbegriffe der Kryptographie

> *Kryptographische Methoden sind mathematisch-logische Techniken zum Schutz von Informationen gegen unbefugte Kenntnisnahme oder unbefugte oder zufällige Manipulation. Sie ergänzen die sonst erforderlichen technisch-organisatorischen Sicherungsmaßnahmen.*

Kryptographische Verfahren basieren vereinfacht gesehen darauf, dass ein mathematisches Problem für befugte BenutzerInnen, die einen „Schlüssel“ (d. i. eine geheime und besondere Information) besitzen (oder wissen), einfach zu lösen ist, während das gleiche Problem ohne den „Schlüssel“ in vertretbarer Zeit NICHT gelöst

werden kann. Ein mathematischer Rechenvorgang, welcher ein kryptographisches Verfahren in konkrete Einzelschritte umsetzt, heißt Algorithmus. In der Praxis werden die Nutzdaten mittels eines solchen Algorithmus in sinnlos erscheinende Zahlen verwandelt (verschlüsselt) und bei Bedarf wieder zurückgerechnet (entschlüsselt).

In der Anwendung verschlüsseln die AbsenderInnen Daten, wenn sie über einen unsicheren Kanal geschickt oder in einer unsicheren Umgebung gespeichert werden sollen. Berechtigte EmpfängerInnen (bzw. die AbsenderInnen) entschlüsseln dann die Daten, wenn sie benötigt werden. In der unsicheren Umgebung sind die verschlüsselten Daten für Unbefugte unleserlich und unbrauchbar.

Ein prinzipielles Problem liegt aber in der stetig zunehmenden Leistungsfähigkeit von Rechnern: Via Internet zu Hunderten oder Tausenden parallel geschaltet, können sie auch scheinbar unlösbare mathematische Probleme durch Ausprobieren aller Möglichkeiten aushebeln, bis sinnvolle Daten aufscheinen (sog. „Brute Force Angriffe“). Dem wird mittels geeigneten (d. h. möglichst langen) Schlüsseln entgegengewirkt.

Kryptographische Grundziele

Man unterscheidet vier kryptographische Grundziele, welche mit kryptographischen Methoden erreicht werden können. Zu ihrer Umsetzung sind immer sowohl technische als auch organisatorsische Maßnahmen erforderlich:

1. Vertraulichkeit (Geheimhaltung): Keine unbefugte dritte Partei soll den Inhalt der Nachricht bzw. Daten lesen bzw. verwerten können.
2. Integrität: Jedwede Manipulationen an den Daten (absichtlich oder durch Übertragungsfehler bedingt) sollen entdeckt werden können.
3. Authentizität:
    - Herkunftsnachweis (Nachrichtenauthentisierung): Ein Absender/eine Absenderin einer Nachricht soll dem Empfänger/der Empfängerin beweisen können, dass sie von ihm stammt und nicht verändert wurde.
    - Damit ist auch ein elektronischer Identitätsnachweis (Authentisierung von Kommunikationspartnern) realisierbar: Eine Kommunikationspartei (z. B. Person, Organisation, IT-System) soll einer anderen ihre Identität zweifelsfrei beweisen können.
4. Nichtabstreitbarkeit (Verbindlichkeit, non repudiation): Die Authentisierung richtet sich an einen oder mehrere Dritte, z. B. bei einem Disput:
    - Nichtabstreitbarkeit der Herkunft: Ein Absender/Eine Absenderin einer bestimmten Nachricht an einen Empfänger/eine Empfängerin soll das Absenden nicht nachträglich bestreiten können.

- Nichtabstreitbarkeit des Erhalts: Ein Empfänger/Eine Empfängerin soll den Erhalt einer bestimmten Nachricht eines bestimmten Absenders/einer bestimmten Absenderin nicht nachträglich bestreiten können.

Dies entspricht Funktionalitäten von Unterschriften.

Die grundlegende kryptographische Methode zur Wahrung von Vertraulichkeit ist **Verschlüsselung**, die grundlegenden Methoden zur Gewährleistung von Integrität, Authentizität und Nichtabstreitbarkeit sind **Hashfunktionen, Message Authentication Codes (MACs), digitale Signaturen** und **kryptographische Protokolle**.
Für Beschreibungen der einzelnen Methoden siehe 10.2 Kryptographische Methoden.

[Quelle: BSI M 3.23]

10.1.1 Entwicklung eines Kryptokonzepts

Aufgrund der Vielfalt kryptographischer Problemstellungen und unterschiedlicher Einflussfaktoren wie IT-System, Datenvolumen, angestrebtes Sicherheitsniveau und Verfügbarkeitsanforderungen gibt es auch vielfältige Lösungsansätze und Realisierungsmöglichkeiten. Um den benötigten Grad an Sicherheit zu erreichen ist es erforderlich, ein Kryptokonzept zu entwickeln, das in das IT-Sicherheitskonzept der Behörde bzw. des Unternehmens integriert wird.

Ein solches Konzept berücksichtigt alle Einflussfaktoren und Entscheidungskriterien für die Wahl eines konkreten kryptographischen Verfahrens und der entsprechenden Produkte. Dazu gehört auch die wirtschaftliche Vertretbarkeit, es fallen Planungs-, Investitions- und laufende Betriebskosten an und die Komplexitiät der Geschäftsabwicklung nimmt zu: So sind etwa Aspekte wie Performance-, Systemanbindungs- oder Interoperabilitäts- und Standardkonformitätsanforderungen betroffen.

Die Auswahl geeigneter kryptographischer Komponenten basiert dann auf diesem Konzept. Das Schlüsselmanagement ist dabei ein besonders kritisches Element im gesamten Kryptokonzept. Konzepte und Lösungsansätze können nur dann erfolgreich erarbeitet und gezielt umgesetzt werden, wenn deutlich wird, welche speziellen Sicherheitsfunktionalitäten bzw. Sicherheitsdienste benötigt werden.

Ein möglicher Aufbau eines Kryptokonzepts ist in B.11 Inhaltsverzeichnis Kryptokonzept (Muster) beispielhaft aufgezeigt.

Jedenfalls muss geklärt und konkret vorgegeben werden,

- welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau es zu erreichen gilt,

- welche finanziellen und personellen Ressourcen zur Verfügung stehen, um die geplanten Sicherheitsmechanismen einzurichten und den Betrieb zu gewährleisten,
- welche Systemanbindung angestrebt wird bzw. welche Einsatzbedingungen für Sicherheitskomponenten vorherrschen,
- welcher Funktions- und Leistungsumfang anzupeilen ist und
- wer letztendlich die Verantwortung übernimmt.

Im Kryptokonzept ist außerdem der technische bzw. organisatorische Einsatz der kryptographischen Produkte zu beschreiben, also z. B.

- ob, wann und wie die Daten verschlüsselt oder signiert werden müssen,
- welche strukturellen Einheiten (Nachrichten, Dateien, Laufwerke) verschlüsselt werden sollen,
- wer welche Zugriffsrechte erhält,
- welche Dienste remote angeboten werden,
- wie die Verwaltung von Passwörtern und Schlüsseln bezüglich Gültigkeitsdauer, Verwendung von Zeichen, Länge und Vergabe gehandhabt werden soll,
- wer mit wem kryptographisch gesichert bzw. ungesichert kommunizieren darf,
- wer bestimmte Rechte vergeben darf usw.

und zwar in Abhängigkeit von den systemtechnischen Rahmenbedingungen bezüglich

- des zu betrachtenden Datenvolumens und der Zeitabhängigkeit,
- der Verfügbarkeitsanforderungen und Gefährdungslage,
- Art und Häufigkeit der zu schützenden Anwendungen etc.

Die jeweiligen Einflussfaktoren für den Einsatz kryptographischer Verfahren sind zu bestimmen und zu dokumentieren (siehe 10.1.2 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte).
Darauf basiert dann die Analyse in Frage kommender Realisierungsmöglichkeiten für konkrete Einsatzbereiche (etwa PC-Arbeitsplatz, Server, LAN-Bereich, Kommunikation), sowie die anschließende Planung für Einführung und Einsatz inkl. formeller Anordnung durch das Management.

Einzelne Punkte dieses Konzepts werden in den nachfolgenden Maßnahmenbeschreibungen näher ausgeführt.

Bei der Erstellung eines Kryptokonzeptes handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Kryptokonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

[Quelle: BSI M 2.161]

10.1.2 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte

Um bei der Verarbeitung und Übertragung sensitiver Informationen zu realistischen, verlässlichen und anwendungsgerechten Bedarfsanforderungen und Rahmenbedingungen für den Einsatz kryptographischer Verfahren und Produkte zu kommen, müssen zunächst die schützenswerten Daten identifiziert und bewertet werden.

Identifikation der zu schützenden Daten

Zunächst muss festgestellt werden, für welche Aufgaben kryptographische Verfahren eingesetzt werden sollen, und welche Daten damit gesichert werden sollen.

Der Einsatz kryptographischer Verfahren kann aus verschiedenen Gründen erforderlich sein, etwa:

- zum Schutz der Vertraulichkeit bzw. der Integrität von Daten,
- zur Authentisierung,
- für Sende- oder Empfangsnachweise.

Je nach Einsatzzweck können verschiedene kryptographische Methoden wie z. B. Verschlüsselung oder digitale Signaturen sinnvoll sein (s. o.).

Um festzustellen, welche kryptographischen Verfahren bzw. Produkte benötigt werden und welche Daten damit zu schützen sind, sollte zunächst die aktuelle IT-Struktur ermittelt werden.

Ermittelt werden sollte,

- welche IT-Systeme es gibt, auf denen Daten verarbeitet bzw. gespeichert (PCs, Notebook, Server, …) oder mit denen Daten übermittelt werden (Bridge, Router, Gateway, Firewall, …) und
- welche Organisationseinheiten und BenutzerInnen die Daten benötigen,
- und welche Datenstrukturen und Übertragungswege es dafür gibt. Dazu sollte die logische und physikalische Vernetzungsstruktur erfasst werden (siehe auch 13.1.2 Ist-Aufnahme der aktuellen Netzsituation).

Schutzbedarf der Daten (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit)

Es sollten alle Anwendungen bzw. Daten ermittelt werden, bei denen ein besonderer Anspruch an Vertraulichkeit, Integrität, Authentizität bzw. Nichtabstreitbarkeit besteht. Allerdings werden nicht nur für IT-Systeme, Anwendungen oder Informationen mit höherem Schutzbedarf kryptographische Produkte benötigt, sondern auch für solche mit mittlerem Schutzbedarf.

Beispiele für Daten mit besonderem Vertraulichkeitsanspruch sind

- personenbezogene Daten,
- Passwörter und kryptographische Schlüssel,
- Daten, aus denen ein Konkurrenzunternehmen finanzielle Gewinne ziehen könnte,
- Daten, ohne deren Vertraulichkeit die Aufgabenerfüllung gefährdet ist (z. B. Ermittlungsergebnisse),
- Daten, deren Veröffentlichung eine Rufschädigung verursachen könnte.

Beispiele für Daten mit besonderem Integritätsanspruch sind

- finanzwirksame Daten, durch deren Manipulation finanzielle Schäden entstehen können,
- Informationen, deren verfälschte Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, deren Verfälschung zu einer verminderten Produktqualität führen kann.

Ein Beispiel für Anwendungen mit besonderem Anspruch an Authentizität sind Fernzugriffe. Ein Beispiel für Daten mit besonderem Anspruch an Nichtabstreitbarkeit sind Bestellungen oder Reservierungen, bei denen die jeweiligen BestellerInnen identifizierbar sein sollten.

Als Ergebnis der Schutzbedarfsfeststellung ist festzulegen, welche Anwendungen oder Daten kryptographisch gesichert werden sollen. Diese Festlegung kann später noch verfeinert werden und sollte regelmäßig überarbeitet werden.

Als Resultat ergibt sich somit ein Überblick über alle Speicherorte und Übertragungsstrecken, die kryptographisch gesichert werden müssen.

Über die sicherheitstechnischen Anforderungen hinaus sind bei der Entwicklung eines Kryptokonzeptes und dem Einsatz kryptographischer Produkte auch noch eine Reihe anderer Aspekte von Bedeutung:

- Technische Aspekte:

Dazu zählen etwa Fragen nach der physischen Sicherheit der Einsatzumgebung und Performance-Anforderungen. Insbesondere ist bei Echtzeit-Daten die Performance trotz Zusatzbelastung durch kryptographische Verarbeitung sicherzustellen.

- Personelle und organisatorische Aspekte:
  Dazu zählen Benutzerfreundlichkeit, Zumutbarkeit und Zuverlässigkeit der kryptographischen Verfahren und Produkte sowie eventueller zusätzlicher Schulungs- und Personalbedarf. Da kryptographische Verarbeitungen Systemressourcen verbrauchen, ist jedenfalls mit spürbaren Auwirkungen auf die Performance zu rechnen. Dazu kommt noch ein gewisser Zeitaufwand für Authentisierung der BenutzerInnen bzw. Start/Beenden der entsprechenden Programme.
- Wirtschaftliche Aspekte:
  Z. B. einmalige Investitionskosten, laufende Kosten für Betrieb und Wartung sowie Lizenzgebühren.
- Key Recovery:
  Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind i. Allg. auch die damit geschützten Daten verloren. Viele Kryptoprodukte bieten daher Funktionen zur Datenwiedergewinnung für solche Fälle an. Solche Funktionen bringen aber auch Risiken mit sich: Wenn dadurch vertrauliche Schlüssel wiederhergestellt werden können, muss sichergestellt sein, dass dies nur Berechtigte können. Wenn es möglich ist, ohne Wissen der Original-Schlüsselbenutzerin bzw. des Original-Schlüsselbenutzers auf deren/dessen Daten zuzugreifen, hat diese/r keine Möglichkeit, böswillige Manipulationen zu beweisen. Der Einsatz von Key Recovery Mechanismen führt auch häufig aufgrund des entgegengebrachten Misstrauens zu Vorbehalten innerhalb des eigenen Unternehmens bzw. Behörde, aber auch bei den Kommunikationspartnern. Bei der Datenübertragung sollte daher generell auf Key Recovery verzichtet werden. Hierfür gibt es auch keine Notwendigkeit, da beim Schlüssel- oder Datenverlust diese einfach noch einmal ausgetauscht werden können. Bei der lokalen Speicherung von Daten sollte der Einsatz sorgfältig überlegt werden (siehe auch 12.4.4 Datensicherung bei Einsatz kryptographischer Verfahren). Bei elektronischen Signaturen ist Key-Recovery generell unzulässig.
- Lebensdauer von kryptographischen Verfahren:
  Kryptographische Verfahren und Produkte müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen. Bereits bei der Auswahl kryptographischer Verfahren sollte daher eine zeitliche Grenze für deren Einsatz festgelegt werden. Zu diesem Zeitpunkt sollte noch einmal gründlich überdacht werden, ob die eingesetzten Kryptomodule noch den erwarteten Schutz bieten.
- Gesetzliche Rahmenbedingungen:

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden, ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und ob für in Frage kommende Produkte Exportbeschränkungen (z. B. lt. Außenhandelsgesetz 1995) beachtet werden müssen (siehe 10.1.4 Auswahl eines geeigneten kryptographischen Produktes).

[Quelle: BSI M 2.163]

10.1.3 Auswahl eines geeigneten kryptographischen Verfahrens

Bevor man sich auf bestimmte kryptographische Verfahren festlegt, sollte man möglichst genaue Vorstellungen haben, welche Ziele (Vertraulichkeit, Integrität, …) auf welchem Niveau in den jeweiligen Anwendungsbereichen damit erreicht werden sollen und mit welchen Eigenschaften dies die unterschiedlichen Verfahren am besten erfüllen können.

Kriterien für die Auswahl eines kryptographischen Verfahrens sind:

- Anwendungs- bzw. Datenstruktur:
  Während sich Integritätsschutz meist und Authentisierung praktisch immer auf kleine Einheiten wie Nachrichten oder Dateien bezieht, besteht bei der Verschlüsselung eine Weichenstellung zunächst darin, ob einzelne Nachrichten (z. B. E-Mail), einzelne Dateien oder ganze Laufwerke (z. B. Festplatten, USB-Sticks) ver- und entschlüsselt werden sollen. Für jeden dieser Anwendungsbereiche existieren spezialisierte Produkte bzw. werden sie auch in Betriebssystemen oder E-Mail-Clients integriert angeboten. Laufwerk-Verschlüsselung eignet sich etwa gut, um Daten bei allfälligem Verlust des Datenträgers (z. B. gestohlenes Notebook) zu schützen, schon aufgrund des Volumens aber nicht, um sie sicher zu versenden.
- Symmetrische, asymmetrische oder hybride Verfahren:
  Aus Performancegründen werden für Verschlüsselungszwecke keine reinen Public-Key-Implementierungen eingesetzt. Alle gängigen Implementierungen von Public-Key-Kryptographie nutzen hybride Verfahren. In Anwendungen mit großen oder offenen Nutzergruppen empfiehlt sich meist die Verwendung eines hybriden Verfahrens (wegen der Vorzüge für das Schlüsselmanagement). Bei kleinen, geschlossenen Nutzergruppen (insbesondere natürlich bei einzelnen BenutzerInnen) kann man sich auf symmetrische Verfahren beschränken. Bei Einsatz hybrider Verfahren ist es sinnvoll, die Stärken des symmetrischen und des asymmetrischen Anteils aufeinander abzustimmen.

Da mit dem asymmetrischen Verfahren vor einem Schlüsselwechsel in der Regel viele Schlüssel für das symmetrische Verfahren verschlüsselt werden („Überschlüsselung“), sollte der asymmetrische Algorithmus mit hinreichenden Schlüssellängen (siehe unten) ausgelegt werden.

Bei der Auswahl von Verfahren und Schlüssellängen sind auch die zunehmenden Bedrohungen durch KI-Systeme zu bedenken. Diese beschränken sich derzeit hauptsächlich auf die Seitenkanalanalyse können in Zukunft aber auch andere Bereiche betreffen. Die Forschung in diesem Bereich fokussiert sich vor allem auf Bedrohungen für symmetrische Verfahren sowie – als positive Erscheinung von KI-Systemen - auf die Sicherheitsbewertung von kryptografischen Verfahren mittels KI.

- Mechanismenstärke / Schlüssellänge:
  Ein wesentliches Kriterium für die Auswahl von kryptographischen Verfahren stellt ihre kryptographische Stärke dar.
  - Bei symmetrischen Verfahren stellt eine ausreichend große Schlüssellänge eine notwendige - wenn auch nicht hinreichende - Bedingung für die Sicherheit dar. Je größer die verwendete Schlüssellänge bei einem kryptographischen Verfahren ist, desto länger dauert die Berechnung des Schlüssels durch eine Brute-Force-Attacke. Andererseits werden die Verfahren bei der Verwendung längerer Schlüssel langsamer, so dass immer zu überlegen ist, welche Schlüssellänge unter Nutzen-/ Leistungsgesichtspunkten angemessen ist. Als Faustregel für gute Verfahren (AES, Serpent, Triple-DES, …) gilt derzeit, dass die eingesetzten Schlüssel mindestens 100 Bit lang sein sollten. (vgl. SOGIS Agreed Cryptographic Mechanisms oder BSI TR-02102-1). Demnach sind aktuell empfohlen:
    - 100 bit - Legacy Standard Level (5 - 10 Jahre voraussichtliche Widerstandsfähigkeit; Triple-DES 2-key),
    - 125 bit - near term protection (10 Jahre),
    - 256 bit - long term protection (10 - 50 Jahre; AES)
  - Blockchiffren sollten generell nurmehr in Kombination mit Datenauthentisierung (Authenticated Encryption with Associated Data - AEAD) eingesetzt werden. Empfohlen werden hierzu derzeit beispielsweise die Verfahren CCM, GCM oder EAX (vgl. SOGIS Agreed Cryptographic Mechanisms). Weitere, nichtmehr empfohlene aber unter Berücksichtigung der Einsatzbedingungen und -beschränkungen einsetzbare Verfahren sind CTR, OFB, CBC und CFB.
  - Hierbei sei auch auf das kryptographische Protokoll TLS zur Absicherung von Datenübertragungen hingewiesen. Derzeit sind die Protokollversionen TLSv1.2 und TLSv1.3 empfohlen. Konkret empfohlene Cipher Suites sind in SOGIS Agreed Cryptographic Mechanisms oder BSI TR-02102-1 aufgelistet.

- Bei asymmetrischen Verfahren sollte die Mechanismenstärke so gewählt werden, dass die Lösung der zu Grunde liegenden mathematischen Probleme zum Brechen des Verfahrens einen unvertretbar großen bzw. praktisch unmöglichen Rechenaufwand erfordert (die zu wählende Mechanismenstärke hängt daher vom aktuellen Stand der Algorithmik und der Leistung der verfügbaren Rechner ab). Gegenwärtig kann man davon ausgehen, dass mit Modullängen von 2048 Bit bei RSA bzw. Untergruppenordnungen in der Größe von 256 Bit bei Elliptischen Kurven ausreichende Sicherheit für *mittleren Schutzbedarf* erreicht wird. Da der Aufwand mit Fortschreiten der Rechentechnik allmählich in den Bereich des technisch Machbaren gerät, sollten die derzeit eingesetzten *legacy* Algorithmen (vgl. SOGIS Agreed Cryptographic Mechanisms) bei Neuentwicklungen nicht mehr verwendet und auf längere Sicht ganz abgelöst werden.
  Für langfristige Sicherheitsanwendungen sollten 15360 Bit RSA-Moduli bzw. Untergruppenordnungen von mindestens 512 Bit eingesetzt werden.
  Für qualifizierte bzw. fortgeschrittene elektronische Signaturen und Siegeln dürfen in der EU nach eIDAS-VO nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs der Verordnung erfüllen. Diese nennt keinen Ablauf der Sicherheitsperiode. Jedoch sind die für die technische Sicherheit der Algorithmen und Parameter geltenden Randbedingungen so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen. Empfehlungen und Prognosen im SOGIS-Kryptokatalog (SOGIS Agreed Cryptographic Mechanisms) sehen für asymmetrische Verfahren folgende Mindestwerte vor, die voraussichtlich auch über das Jahr 2027 hinaus noch als Stand der Technik gelten:

  - RSA: mindestens 3000 Bit
  - FF-DLOG: mindestens 3000 Bit
  - EC-DLOG: mindestens 256 Bit
- Grundsätzlich sollten nur Algorithmen eingesetzt werden, die veröffentlicht sind, von einem breiten Fachpublikum intensiv untersucht wurden und von denen keine Sicherheitslücken bekannt sind. Vor der Verwendung von unbekannten Algorithmen aus Quellen, deren kryptographische Kompetenz nicht ausreichend nachgewiesen ist, kann nur gewarnt werden.

- Realisierbarkeit von technischen Anforderungen
  Die Verschlüsselungsalgorithmen müssen so beschaffen sein, dass die technischen Anforderungen, insbesondere die geforderte Performance, durch eine geeignete Implementation erfüllt werden können. Hierunter fallen Anforderungen an die Fehlerfortpflanzung (z. B. falls über stark rauschende Kanäle gesendet wird), aber auch Anforderungen an Synchronisationsoverhead und Zeitverzögerung (z. B. falls „Echtzeit“-Verschlüsselung von großen Datenmengen erforderlich ist).

10.1.4 Auswahl eines geeigneten kryptographischen Produktes

Aufgrund des breiten Spektrums kryptographischer Anwendungen können im Folgenden lediglich grundsätzliche Empfehlungen zur Auswahl von kryptographischen Produkten gegeben werden, die im konkreten Fall zu detaillieren sind.

Anwendungs- bzw. Datenstruktur:

Das ausgewählte Produkt muss sich selbstverständlich zunächst nach den verwendeten Anwendungs- und Datenstrukturen richten, also Integritätsschutz oder Authentisierung bzw. Ver- und Entschlüsselung von Nachrichten (z. B. E-Mail), einzelnen Dateien oder ganzer Laufwerke (z. B. Festplatten, USB-Sticks) unterstützen. Es gibt kaum Produkte, die für alle Anwendungsbereiche gleichermaßen geeignet sind; andererseits werden sie mitunter bereits in Betriebssystemen oder E-Mail-Clients integriert angeboten. In diesem Fall muss besonders darauf geachtet werden, dass sie die notwendigen Mindeststärken erreichen. Das ist etwa bei Produkten US-amerikanischer Herkunft nicht immer der Fall.

Funktionalität

Das ausgewählte Produkt muss die von den AnwenderInnen spezifizierte Funktionalität aufweisen.

Es muss insbesondere:

- die geforderten kryptographischen Grunddienste leisten,
- evtl. besonderen Anforderungen durch die Einsatzumgebung genügen (z. B. Single-User/Multi-User-PC, LAN-Umgebung, WAN-Anbindung),
- die geforderten technischen Leistungsmerkmale aufweisen (z. B. Durchsatzraten),
- die geforderten Sicherheitsfunktionalitäten aufweisen, insbesondere müssen die eingesetzten kryptographischen Mechanismen die erforderliche Stärke aufweisen.

Interoperabilität

Das ausgewählte Produkt wird in der Regel in eine bestehende IT-Umgebung eingefügt.

Es muss dort möglichst interoperabel sein. Die Einhaltung interner Standards ist nötig, um die Interoperabilität mit dem bereits vorhandenen IT-System bzw. Systemkomponenten zu gewährleisten. Die Anwendung internationaler Standards für kryptographische Techniken sollte selbstverständlich sein, sie erleichtert auch eine Sicherheitsevaluierung der kryptographischen Komponenten.

Wirtschaftlichkeit

Das ausgewählte Produkt sollte möglichst wirtschaftlich sein.

Dabei müssen Anschaffungskosten, Stückzahlen, Kosten für Wartung und Produktpflege, aber auch Einsparungen durch etwaige Rationalisierungseffekte berücksichtigt werden.

Zertifizierte Produkte

Die „Information Technology Security Evaluation Criteria“ [ITSEC] bzw. die „Common Criteria“ [Common Criteria] bieten einen Rahmen, innerhalb dessen die Sicherheitsfunktionalitäten eines IT-Produktes durch Anlegen von etablierten Kriterien in eine genau spezifizierte Hierarchie von Sicherheitsstufen eingeordnet werden können.

Die Informationssicherheitsbehörden mehrerer Staaten haben jeweils ein nationales Zertifizierungsschema nach diesen Kriterien aufgebaut.

Der Einsatz eines zertifizierten Produktes bietet die Gewähr, dass die Sicherheitsfunktionalität dieses Produktes unabhängig geprüft wurde und den im Evaluationslevel spezifizierten Standard nicht unterschreitet (siehe auch 14.2.1 Beachtung des Beitrags der Zertifizierung für die Beschaffung).

Importprodukte

In mehreren Staaten unterliegt der Export von starker Kryptographie starken Beschränkungen.

Insbesondere wird die Stärke von an sich starken Verschlüsselungsprodukten künstlich (durch Reduzierung der Schlüsselmannigfaltigkeit) herabgesetzt. Solche künstlich geschwächten Verfahren erreichen i. d. R. nicht die für mittleren Schutzbedarf erforderliche Mechanismenstärke. Beim Einsatz von Importprodukten sollte immer darauf geachtet werden, ob sie den vollen Leistungsumfang bieten.

Grenzüberschreitender Einsatz

Viele Unternehmen und Behörden haben zunehmend das Problem, dass sie auch ihre internationale Kommunikation, z. B. mit ausländischen Tochterunternehmen, kryptographisch absichern wollen.

Hierfür muss zunächst untersucht werden,

- ob innerhalb der jeweiligen Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und
- ob für in Frage kommende Produkte Export- oder Importbeschränkungen bestehen.

Fehlbedienungs- und Fehlfunktionssicherheit

Das Gefährliche an kryptographischen Produkten ist, dass sie AnwenderInnen in einer - mitunter trügerischen - Sicherheit wiegen.

Daher kommt Maßnahmen gegen Kompromittierungen durch Bedienungsfehler oder technisches Versagen besondere Bedeutung zu, da deren Folgen eine gravierende Gefährdung der Sicherheit darstellen können. Allerdings ist die Bandbreite bezüglich redundanter Systemauslegung und zusätzlicher Überwachungsfunktionen - und damit an Gerätekosten - groß, sodass hier die Maßnahmen im Einzelfall in Abhängigkeit von den Anforderungen festzulegen sind.

Implementierung in Soft-, Firm- oder Hardware

Kryptographische Algorithmen können sowohl in Software, in Firmware als auch in Hardware implementiert werden.

Softwarerealisierungen werden in der Regel vom Betriebssystem des jeweiligen IT-Systems gesteuert. Unter Firmware versteht man Programme und Daten, die permanent so in Hardware gespeichert sind, dass die Speicherinhalte nicht dynamisch verändert werden können, und die während ihres Ablaufs nicht modifiziert werden können. Bei Hardwarelösungen wird das kryptographische Verfahren direkt in Hardware realisiert, z. B. als separates Sicherheitsmodul oder als Einsteckkarte.

Softwarelösungen bieten den Vorteil, leicht anpassbar und kostengünstig zu sein. Hardwarerealisierungen bieten i. Allg. sowohl höhere Manipulationsresistenz (und damit Sicherheit) als auch höheren Datendurchsatz als Softwarerealisierungen, sie sind aber meist auch teurer.

Firmwarelösungen kann man als Kompromiss der beiden vorangegangenen Möglichkeiten verstehen. Die Vor- und Nachteile der jeweiligen Realisierung beziehen sich jedoch immer nur auf lokale Aspekte (dazu gehört vor allem das Schlüsselmanagement). Sind die Daten einmal verschlüsselt und befinden sie sich auf dem Kommunikationsweg, ist im Prinzip das Zustandekommen der Verschlüsselung nicht mehr relevant.

Ein Beispiel für (relativ) preiswerte, transportable und benutzerfreundliche Kryptomodule sind Chipkarten, die im Bereich der lokalen Verschlüsselung als sicheres Speichermedium für die kryptographischen Schlüssel oder im Bereich der Authentikation zur Passwort-Generierung und Verschlüsselung eingesetzt werden können.

10.1.5 Regelung des Einsatzes von Kryptomodulen

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von Kryptomodulen gestellt werden. Diese müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden.

Wichtige organisatorische Regelungen dafür sind:

- Es müssen Verantwortliche benannt werden, und zwar für die Erstellung des Kryptokonzeptes, für die Auswahl sowie für den sicheren Betrieb der kryptographischen Produkte.
- Es sind geeignete personelle Maßnahmen festzulegen bzw. durchzuführen (Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen).
- Die BenutzerInnen sollten nicht nur im Umgang mit den von ihnen zu bedienenden Kryptomodulen geschult werden, sie sollten darüber hinaus für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und einen Überblick über kryptographische Grundbegriffe erhalten.
- Falls Probleme oder der Verdacht auf Sicherheitsvorfälle beim Einsatz von Kryptomodulen auftreten, muss klar definiert sein, was in solchen Fällen zu unternehmen ist. Alle BenutzerInnen müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.
- Im Rahmen des Kryptokonzeptes ist festzulegen, wer wann welche Kryptoprodukte benutzen muss bzw. darf und welche Randbedingungen dabei zu beachten sind (z. B. Schlüsselhinterlegung).
- Der korrekte Einsatz der Kryptomodule sollte regelmäßig überprüft werden. Ebenso ist regelmäßig zu hinterfragen, ob die eingesetzten kryptographischen Verfahren noch dem Stand der Technik entsprechen.
- Abhängig von den definierten Verfügbarkeitsanforderungen sollten Ersatz-Kryptomodule vorrätig gehalten werden, um einen reibungslosen Betrieb zu gewährleisten. Dies ist insbesondere dort wichtig, wo der Zugriff auf verschlüsselte Daten von der Funktionsfähigkeit eines einzelnen Kryptomoduls abhängt, z. B. bei der Datenarchivierung oder der Leitungsverschlüsselung.

Zur Gewährleistung eines sicheren Betriebs der Kryptomodule sind folgende Maßnahmen zu setzen:

- Vor der Inbetriebnahme muss die optimale Konfiguration der Kryptomodule festgelegt werden, z. B. hinsichtlich Schlüssellänge, Betriebsmodi oder Kryptoalgorithmen.
- Die festgelegte Konfiguration muss dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.

- Für die BenutzerInnen müssen die Kryptoprodukte durch die AdministratorInnen so vorkonfiguriert sein, dass ohne weiteres Zutun der BenutzerInnen maximale Sicherheit erreicht werden kann.
- Bei komplexeren Kryptoprodukten müssen geeignete Handbücher verfügbar sein.
- Die Kryptomodule müssen sicher installiert und anschließend getestet werden.
- Die Anforderungen an die Einsatzumgebung müssen festgelegt sein, eventuell sind dafür ergänzende Maßnahmen im IT-Umfeld zu treffen.
- Umfang und Häufigkeit der Wartung sowie die Verantwortlichkeiten dafür sind festzulegen.

10.1.6 Physikalische Sicherheit von Kryptomodulen

Wie in 10.1.4 Auswahl eines geeigneten kryptographischen Produktes beschrieben, können Kryptomodule in Soft-, Firm- oder Hardware realisiert sein. Die Umsetzung in Hardware wird insbesondere dann gewählt, wenn das Kryptomodul besonders manipulationsresistent sein soll.

Hardware-Kryptomodule sollten unter Verwendung von physikalischen Sicherheitsmaßnahmen oder unter Ausnutzung entsprechender Materialeigenschaften so konstruiert sein, dass ein unautorisierter physikalischer Zugriff auf Modulinhalte erfolgreich verhindert werden kann.

Möglichkeiten dazu sind etwa:

- die Verwendung von Passivierungsmaterialien,
- geeignete Tamperschutzmaßnahmen,
- mechanische Schlösser sowie
- automatische Löschung (Vernichtung) aller im Klartext enthaltenen sensitiven Schlüsseldaten und -parameter bei unbefugtem Öffnen des Gehäuses.

Durch den Einsatz von Sensoren und Überwachungseinrichtungen lässt sich sicherstellen, dass das Kryptomodul in seinem vorgesehenen Arbeitsbereich, etwa bzgl. Spannungsversorgung, Taktung, Temperatur, mechanische Beanspruchung und elektromagnetische Beeinträchtigung, betrieben wird.

Zur Aufrechterhaltung seiner beabsichtigten Funktionalität sollte das Kryptomodul Selbsttests initiieren und durchführen können. Diese Tests können sich auf folgende Bereiche erstrecken: Algorithmentests, Soft- und Firmwaretests, Funktionstests, statistische Zufallstests, Konsistenztests, Bedingungstests sowie Schlüsselgenerierungs- und -ladetests. Bei einem negativen Testergebnis sollte den BenutzerInnen des Kryptomoduls eine entsprechende Fehlermeldung signalisiert und ein entsprechender Fehlerzustand eingenommen werden. Erst nach Behebung der Fehlerursache(n) darf eine Freischaltung aus diesem Fehlerzustand möglich sein.

Beim Einsatz von Softwareprodukten muss die physikalische Sicherheit des Kryptomoduls durch das jeweilige IT-System bzw. dessen Einsatzumgebung geleistet werden. Eine Softwarelösung sollte Selbsttests durchführen können, um Modifikationen durch Trojanische Pferde oder Viren erkennen zu können.

10.1.7 Schlüsselmanagement

Bei jedem Einsatz von Verschlüsselung entsteht die Aufgabe, die Schlüssel angemessen zu verwalten. Es stellt sich die Frage, wie man

- Erzeugung/Initialisierung,
- Vereinbarung/Etablierung,
- Verteilung/Transport,
- Wechsel/Update,
- Speicherung,
- Beglaubigung/Zertifizierung,
- Rückruf,
- Wiedergewinnung im Fall von Vernichtung/Verlust,
- Vernichtung/Löschen,
- Archivierung

während des gesamten Lebenszyklus der Schlüssel durchführt. Das Schlüsselmanagement kann und wird sich gewöhnlich auch kryptographischer Techniken bedienen. Es muss für die Gesamtheit der Kryptomodule eines kryptographisch basierten Sicherungssystems durchgeführt werden. Geheime Schlüssel müssen vor unbefugter Aufdeckung, Modifizierung und Ersetzung geschützt werden. Öffentliche Schlüssel müssen vor unbefugter Modifizierung und Ersetzung geschützt werden.

Angemessenes Schlüsselmanagement ist die Voraussetzung dafür, dass Information durch kryptographische Methoden überhaupt geschützt werden kann. Schlüsselmanagement benötigt eigens dieser Aufgabe gewidmete Ressourcen!

[Quelle: BSI M 3.23]

Die Verwendung kryptographischer Sicherheitsmechanismen (z. B. Verschlüsselung, digitale Signatur) setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus. Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder gar aus unkontrollierter Quelle stammen, können den kryptographischen Sicherheitsmechanismus genauso kompromittieren wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Qualitativ gute Schlüssel werden in der Regel unter Verwendung geeigneter Schlüsselgeneratoren erzeugt.

Für das Schlüsselmanagement sind folgende Punkte zu beachten:

Schlüsselgenerierung

Die Auswahl der Schlüssel muss sich am eingesetzten Verfahren orientieren.

Schlüssel dürfen nicht leicht erratbar oder rekonstruierbar sein. Für eine „gute“ Schlüsselwahl eignen sich insbesondere Zufallszahlengeneratoren. Auch muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens etwaige voreingestellte Schlüssel geändert werden.

Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptographische Schlüssel können zum einen direkt am Einsatzort (und dann meistens durch die BenutzerInnen initiiert) oder zum anderen zentral erzeugt werden. Bei der Erzeugung vor Ort müssen meistens Abstriche an die Sicherheit der Umgebung gemacht werden. Bei zentraler Schlüsselgenerierung muss sichergestellt sein, dass sie ihre BesitzerInnen authentisch und kompromittierungsfrei erreichen.

Geeignete Schlüsselgeneratoren müssen kontrollierte, statistisch gleichverteilte Zufallsfolgen unter Ausnutzung des gesamten möglichen Schlüsselraums produzieren. Dazu erzeugt z. B. eine Rauschquelle zufällige Bitfolgen, die mit Hilfe einer Logik nachbereitet werden. Anschließend wird unter Verwendung verschiedener Testverfahren die Güte der so gewonnenen Schlüssel überprüft.

Einige Kryptomodule, insbesondere solche, die keinen integrierten Zufallszahlengenerator besitzen, greifen auf Benutzereingaben zur Schlüsselerzeugung zurück. Beispielsweise werden hier Passwörter abgefragt, aus denen dann ein Schlüssel abgeleitet wird, oder die BenutzerInnen werden gebeten, beliebigen Text einzutippen, um zufällige Startwerte für die Schlüsselgenerierung zu erhalten. Solche Passwörter sollten dabei gut gewählt sein und möglichst lang sein. Wenn möglichst „zufällige“ Benutzereingaben angefordert werden, sollten diese auch zufällig, also schlecht vorhersagbar, sein.

Schlüsseldiversifizierung

Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen.

Insbesondere sollten für die Verschlüsselung immer andere Schlüssel als für die Signaturbildung benutzt werden. Dies ist sinnvoll,

- damit bei der Offenlegung eines Schlüssels nicht alle Verfahren betroffen sind,
- um Abhängigkeiten zwischen Schlüsseln bzw. erzeugten Daten zu vermeiden,
- da es manchmal erforderlich sein kann, Schlüssel weiterzugeben (Vertretungsfall),
- da es unterschiedliche Zyklen für den Schlüsselwechsel geben kann.

Schlüsselverteilung/Schlüsselaustausch

Kryptographische Kommunikationsbeziehungen können nur dann funktionieren, wenn die Kommunikationspartner über aufeinander abgestimmte kryptographische Schlüssel verfügen.

Dazu müssen alle Kommunikationspartner mit den dazu erforderlichen Schlüsseln versorgt werden. Zur Schlüsselverteilung und zum Schlüsselaustausch können unterschiedliche Verfahren verwendet werden.

Unter Schlüsselverteilung wird hier die initiale Versorgung der Kommunikationspartner mit Grundschlüsseln verstanden. Die Schlüssel werden dazu von einer meist zentralen Schlüsselerzeugungsstelle (z. B. einem Trust Center) an die einzelnen Kommunikationspartner übermittelt. Die Verteilung der Schlüssel sollte auf geeigneten Datenträgern (z. B. Chipkarten) oder über Kommunikationsverbindungen (z. B. LAN, WAN) vertraulich (z. B. verschlüsselt), integer (z. B. MAC-gesichert) und authentisch (z. B. digital signiert) erfolgen. Die unbefugte Kenntnisnahme bzw. Verfälschung der Schlüssel muss verhindert oder wenigstens erkannt werden können.

Mit Schlüsselaustausch wird die Schlüsseleinigungsprozedur zwischen zwei Kommunikationspartnern auf einen Sitzungsschlüssel (Session Key) bezeichnet. Der Session Key ist ein Schlüssel, der nur eine begrenzte Zeit, etwa für die Dauer einer Kommunikationsverbindung, verwendet wird. Diese Zeit muss festgelegt werden, da Sitzungen sehr lange dauern können. Die Festlegung erfolgt z. B. durch einen relativen Zeitablauf oder durch einen Paketzähler. Für jede neue Verbindung wird ein neuer Session Key zwischen den Kommunikationspartnern ausgehandelt.

Moderne Systeme bedienen sich heute asymmetrischer kryptographischer Verfahren zur Schlüsselverteilung und zum Schlüsselaustausch. Zum Nachweis der Authentizität der öffentlichen Schlüssel kann eine vertrauenswürdige Zertifizierungsstelle verwendet werden. Dies ist etwa auch auf der österreichischen Bürgerkarte realisiert.

Schlüsselinstallation und -speicherung

Im Zuge der Schlüsselinstallation ist die authentische Herkunft sowie die Integrität der Schlüsseldaten zu überprüfen. Generell sollten Schlüssel nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Bei Softwareverschlüsselungsprodukten muss berücksichtigt werden, dass Schlüssel zumindest zeitweise während des Ver-/Entschlüsselungsprozesses in Klarform im PC-System vorliegen müssen.

Der Vertraulichkeitsschutz durch Verschlüsselung kann nur dann umfassend erreicht werden, wenn die verwendeten kryptographischen Schlüssel geheim gehalten werden können.

Bieten die IT-Systeme, auf denen das Verschlüsselungsverfahren eingesetzt ist, keinen ausreichenden Zugriffsschutz für die Schlüssel, sollten diese nicht auf diesem IT-System gespeichert werden. Besser ist eine bedarfsorientierte manuelle Eingabe oder die Auslagerung der Schlüssel auf einen externen Datenträger. Aus Sicherheitsgründen bieten sich hier insbesondere Chipkarten an.

Auf jeden Fall muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.

Schlüsselarchivierung

Für Archivierungszwecke sollte das kryptographische Schlüsselmaterial auch außerhalb des Kryptomoduls in verschlüsselter Form speicherbar und gegebenenfalls wieder einlesbar sein.

Die kryptographischen Schlüssel können ihrerseits wieder - unter einem so genannten Masterkey oder Key-Encrypting-Key (KEK) - verschlüsselt werden. Der KEK muss entsprechend sicher (z. B. auf einer im Safe deponierten Chipkarte gespeichert) aufgehoben werden. Empfehlenswert ist die Splittung des KEK in zwei oder mehrere Teilschlüssel, sodass zur Rekonstruktion des KEK zwei oder mehrere Personen gleichzeitig anwesend sein müssen.

Im Bereich der öffentlichen Verwaltung wird zur Verschlüsselung die Verwendung von Verschlüsselungszertifikaten empfohlen, wobei alle Zertifikate innerhalb einer Organisationseinheit das gleiche Schlüsselpaar verwenden, sodass eine separate Schlüsselhinterlegung nicht notwendig wird. Es ist somit nur mehr das innerhalb der Organisationseinheit gemeinsame Schlüsselpaar geeignet zu archivieren (vgl. [IKTB-181202-1]).

Zugriffs- und Vertretungsregelung

In der Sicherheitspolitik sollten Fragen bzgl. der Zugriffs- und Vertretungsrechte geregelt sein.

Entsprechende Mechanismen müssen vom Schlüsselmanagement und von den einzusetzenden Kryptomodulen/-geräten unterstützt werden (z. B. Schlüsselhinterlegung für den Fall, dass MitarbeiterInnen das Unternehmen verlassen oder wegen Krankheit längere Zeit ausfallen).

Wird innerhalb einer Organisationseinheit der öffentlichen Verwaltung ein und dasselbe Schlüsselpaar zur Verschlüsselung verwendet, so werden die Vertretungsregeln damit umsetzbar und eine Schlüsselhinterlegung innerhalb einer Einheit wird obsolet (vgl. [IKTB-181202-1]).

Schlüsselwechsel

Die verwendeten Schlüssel sind abhängig von der Häufigkeit ihres Einsatzes, von dem relevanten Bedrohungspotenzial und der Sicherheit ihrer lokalen Aufbewahrung hinreichend oft präventiv zu wechseln.

Im Kryptokonzept muss basierend auf der Sicherheitsrichtlinie festgelegt werden, wann und wie oft Schlüssel gewechselt werden müssen. Je größer die Menge verschlüsselter Daten ist, die einem Angreifer für eine Analyse zur Verfügung steht, um so größer ist bei manchen Verfahren die Chance, dass das Analyseverfahren erfolgreich ist.

Ein regelmäßiger Schlüsselwechsel minimiert die Angriffsmöglichkeiten auf verschlüsselte Daten. Die Wechselfrequenz ist von verschiedenen Faktoren abhängig, wie etwa die Art des verschlüsselten Mediums (z. B. Langzeitdatenträger, Datenübertragungsmedium) oder der kryptographische Algorithmus, die Erkennung von Angriffen (z. B. Diebstahl oder Verlust eines Schlüssels) und die Schutzwürdigkeit der Daten. Weitere Faktoren bei der Festlegung der Wechselfrequenz sind die Häufigkeit des Schlüsseleinsatzes, das relevante Bedrohungspotenzial und die Sicherheit der lokalen Aufbewahrung der Schlüssel.

Bei einigen Verfahren sind für jede einzelne Kommunikationsverbindung jeweils neue Schlüssel auszuhandeln, also Sitzungsschlüssel (Session Keys) zu verwenden. Dies sollte in der Regel für die BenutzerInnen unbemerkt und ohne ihr Zutun durch die Verfahren geschehen. Schlüsselwechsel bedeutet hierbei den Austausch der Masterkeys, die die Grundlage für die jeweils gebildeten Sitzungsschlüssel gebildet werden, und sollte natürlich auch regelmäßig durchgeführt werden.

Besteht der Verdacht, dass ein verwendeter Schlüssel kompromittiert wurde, so ist dieser Schlüssel nicht mehr zu verwenden und alle Beteiligten sind zu informieren. Bereits mit diesem Schlüssel verschlüsselte Informationen sind zu entschlüsseln und mit einem anderen Schlüssel zu verschlüsseln.

Außerbetriebnahme

Nicht mehr benötigte Schlüssel (z. B. Schlüssel, deren Gültigkeitsdauer abgelaufen ist) sind auf sichere Art zu löschen bzw. zu vernichten (z. B. durch mehrfaches Löschen/Überschreiben oder die mechanische Zerstörung des Datenträgers).

Auf Produkte mit unkontrollierbarer Schlüsselablage sollte generell verzichtet werden.

10.1.8 Einsatz elektronischer Signaturen und Siegel

Technisch gesehen stellen elektronische Signaturen und elektronische Siegel die Integrität und Authentizität zu übermittelnder Daten sicher. In Kombination mit einer Hashfunktion können sie von den EmpfängerInnen entsprechend überprüft werden. Mit einem qualifizierten Zertifikat, welches den Signator (BenutzerInnen, welche die elektronische Signatur anbringen) identifiziert, stellen „Qualifizierte Elektronische Signaturen“ ein Äquivalent zur eigenhändischen Unterschrift dar, welches rechtlich auch als solches anerkannt wird.

Qualifizierte elektronische Signaturen müssen auf einem qualifizierten Zertifikat für elektronische Signaturen basieren und von einer sogenannten Qualifizierten Signaturerstellungseinheit (QSEE) erstellt werden. Eine QSEE ist wiederum eine Hardware oder Software die die Anforderungen des Anhangs II aus der Verordnung (EU) Nr. 910/2014 (eIDAS-VO) erfüllt und als solche bescheinigt wurde. Eine einfachere Art der qualifizierten elektronischen Signatur ist die „Fortgeschrittene Elektronische Signatur“. Für sie ist keine QSEE nötig, sie erfüllt dadurch aber auch nichtmehr die Anforderungen um einer eigenhändigen Unterschrift gleichgesetzt zu werden. Elektronische Signaturen können nur natürlichen Personen zugeordnet werden, das Pendant für juristische Personen ist das elektronische Siegel.

Elektronische Signaturen und Siegel leisten im Wesentlichen also zwei Aufgaben:

- Authentifizierung:
  Es kann eindeutig verifiziert werden, ob eine bestimmte Person eine bestimmte elektronische Signatur erzeugt hat bzw. ob ein bestimmtes elektronisches Siegel einer bestimmten juristischen Person zugeordnet ist.
- Überprüfung der Integrität der signierten Daten:
  Es ist eindeutig überprüfbar, ob die Daten, an die eine elektronische Signatur bzw. ein Siegel angehängt wurde, identisch sind mit den Daten, die tatsächlich signiert wurden.

Elektronische Signaturen und Siegel gewährleisten **nicht** die Vertraulichkeit von Daten, hierzu sind zusätzliche Verschlüsselungsmaßnahmen erforderlich.

Allgemein empfiehlt sich der Einsatz elektronischer Signaturen und Siegel vor allem in offenen Systemen, in denen a priori kein gegenseitiges Vertrauen zwischen den KommunikationsteilnehmerInnen vorausgesetzt werden kann, aber verbindliche, authentische Kommunikation erforderlich ist.

In Österreich und auch anderen Ländern dienen qualifizierte elektronische Signaturen als Unterschriftsäquivalent im E-Government und E-Banking. Dabei wird die Signatur jeweils in einer Chipkarte (der „Bürgerkarte“) oder in einem geschützten Modul ausgelöst und mit den Nutzdaten zum Empfänger (z. B. einem amtlichen Portal oder einer E-Banking-Anwendung) geschickt. Nach erfolgreicher Prüfung mit Hilfe des qualifizierten Zertifikats werden die Daten dann verarbeitet. Behörden können dann die Erledigung ebenso elektronisch, mit einer „Amtssignatur“ (diese enthält auch eine Bildmarke) versehen, an den Antragsteller/die Antragstellerin senden.

Siehe zu dieser umfangreichen Materie:

- Bürgerkarte: Ihre persönliche Unterschrift im Internet: Handy und Karte
- [IKTB-090204-03]
- [IKTB-240304-03]

Der rechtliche Rahmen für die Erstellung und Verwendung elektronischer Signaturen und Siegel sowie die Erbringung von Signatur- und Vertrauensdiensten wird EU-weit durch die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-VO) geregelt und in Österreich durch das Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) sowie die zugehörige Signatur- und Vertrauensdiensteverordnung (SVV) ergänzt.

Geregelt wird dort u. a.

- die Rechtswirkungen qualifizierter elektronischer Signaturen,
- Pflichten von Signatoren und Siegelerstellern,
- die Tätigkeiten und Pflichten der Vertrauensdiensteanbieter,
- die Aufsicht.

Aufsichtsstelle ist lt. §12 SVG die Telekom-Control-Kommission (§195 Telekommunikationsgesetz 2021), die sich bei der Durchführung der Aufsicht der Rundfunk und Telekom Regulierungs-GmbH (RTR) bedienen kann.

Als erste Bestätigungsstelle lt. §7 SVG wurde durch Verordnung des Bundeskanzlers vom 02.02.2000 der Verein „Zentrum für sichere Informationstechnologie - Austria (A-SIT)“ (Verordnung - A-Sit) anerkannt.

Adressen und Webseiten siehe F Wichtige Adressen.

10.1.9 Vertrauensdienste

Vertrauensdiensteanbieter

Vertrauensdiensteanbieter (Trust Center) werden immer dann benötigt, wenn asymmetrische Kryptoverfahren wie bei digitalen Signaturen für eine nicht mehr überschaubare Anzahl von Teilnehmern eingesetzt werden. Will man nun die Echtheit der öffentlichen Schlüssel und die sichere Zuordnung der Schlüssel zu Personen sicherstellen, bedarf es der bereits erwähnten Trust Center/ Vertrauensdienste, die die Zuordnung einer Person zu einem öffentlichen Schlüssel durch ein Zertifikat bestätigen.

Durch solche Vertrauensdienste werden typischerweise folgende Aufgaben wahrgenommen:

- Schlüsselgenerierung: Es sind für den Vertrauensdienst und ggf. für Teilnehmer Schlüsselpaare zu generieren.
- Schlüsselzertifizierung: Die Teilnehmerdaten, der korrespondierende öffentliche Schlüssel und weitere Daten werden zu einem Zertifikat zusammengefasst und vom Vertrauensdienst digital signiert.
- Personalisierung: Das Zertifikat und ggf. öffentlicher und privater Schlüssel werden auf eine Signaturkomponente (z.B. eine Chipkarte) übertragen.
- Identifizierung und Registrierung: Die Teilnehmer werden gegen Vorlage eines Ausweispapieres identifiziert und registriert.
- Verzeichnisdienst: Zertifikate werden in einem öffentlichen Verzeichnis abrufbar gehalten. Darüber hinaus muss der Verzeichnisdienst Auskunft darüber geben, ob ein Zertifikat gesperrt ist oder nicht.
- Zeitstempeldienst: Für bestimmte Daten kann es notwendig sein, diese mit einem vertrauenswürdigen Zeitpunkt zu verknüpfen. Dazu wird der Zeitpunkt an die Daten angehängt und das Ergebnis vom Zeitstempeldienst digital signiert.

Im Rahmen der eIDAS-VO (Verordnung (EU) Nr. 910/2014) wurden noch weitere Vertrauensdienste definiert:

- Zustelldienst für elektronische Einschreiben: Nachweisliche Versendung und Empfang elektronischer Zustellstücke.
- Validierungsdienst für elektronische Signaturen und Siegel: Bestätigung der Gültigkeit einer elektronischen Signatur oder Siegels.

- Bewahrungsdienst für elektronische Signaturen und Siegel: Langzeitarchivierung elektronischer Signaturen, Siegeln oder Zertifikate, um langfristig Aussagen zu deren Gültigkeit treffen zu können.

Trust Center können außerdem zusätzlich Schlüsselaufbewahrung als Dienstleistung anbieten, wenn die kryptographischen Schlüssel für Verschlüsselung eingesetzt werden sollen. Um bei Schlüsselverlust noch auf die verschlüsselten Daten zugreifen zu können, kann dann der Schlüsselbesitzer (und nur dieser) eine Schlüsseldublette erhalten, die im Trust Center geschützt aufbewahrt wird. [Quelle: BSI M 3.23]

Zertifikate können einerseits zur Verschlüsselung aber andererseits auch zur Authentisierung verwendet werden. Demnach unterscheiden sich auch die Vorgaben und Anforderungen an die ausstellenden Vertrauensdienste.

Im Rahmen des IKT-Board-Beschlusses vom 11.03.2003 [IKTB-110303-1] wurde die Kennzeichnung von Sicherheitszertifikaten beschlossen. Zur eindeutigen Erkennung von Zertifikaten für Signatur und Server wurde der „Object Identifier“ für .gv.at mit der Arbeitsgruppe der Länder abgestimmt. Zur Stärkung des Vertrauens und zur nachweisbaren Sicherheit wird empfohlen, die Server für Anwendungen des E-Government automatisiert erkennbar zu machen. Dies erfordert die Anwendung der „Richtlinien für Zertifikate für das E-Government“ [IKT-ZERT]. Diese Kennung wurde auch im internationalen Kennungsschema (Zertifikatsattribute) festgelegt.

Im IKT-Board-Beschluss vom 03.05.2005 [IKTB-030505-01] werden für Anwendungen in der Bundesverwaltung je nach Anwendungsgebiet drei Arten von Zertifikaten unterschieden:

- Amtssignatur (automatisch ausgehende Erledigungen und Bescheide)
- Signatur mit der Bürgerkarte/Dienstkarte (Identifikation der Organverwalter und gegebenenfalls, wie die Amtssignatur, für individuelle einzelne Erledigungen)
- Signatur im Rahmen des E-Mailverkehrs

Des Weiteren wurde in [IKTB-110303-2] für eine automatisierte Vernetzung von E-Government-Anwendungen ein eindeutiges Kennzeichen für Organisationseinheiten der öffentlichen Verwaltung (VKZ) empfohlen. Da bereits eine Reihe von Schlüsselsystemen für Teilbereiche der öffentlichen Verwaltung besteht, soll ein Überbau über bestehende Systeme geschaffen werden.

Das Kennzeichen soll für folgende Bereiche verwendet werden:

- Portalverbund,
- Vernetzung von Verfahrensinformationen,
- Verzeichnisdienste und
- elektronische Signatur (Zeichnungsberechtigungen).

Die Verwaltung des Kennzeichens für Teilbereiche der dargestellten Organisationen soll durch diese selbst dezentral erfolgen können.

10.2 Kryptographische Methoden

Da der Einsatz von kryptographischen Systemen bzw. Produkten für die BenutzerInnen zusätzlichen Aufwand bedeuten oder - je nach Komplexität - sogar vertiefte Kenntnisse erfordern kann, wird in der Folge ein Einführungstext zum grundlegenden Verständnis der kryptographischen Mechanismen angeboten.

10.2.1 Elemente der Kryptographie

Mathematische Methoden und Techniken, die zum Schutz von Information gegen unbefugte Kenntnisnahme oder absichtliche Manipulation dienen können, nennt man kryptographisch. Der Schutz der Information durch kryptographische Methoden ist - im Unterschied zu infrastrukturellen und technischen Sicherungsmaßnahmen - mathematisch-logischer Natur.

Bei kryptographischen Verfahren wird ein mathematischer Rechenvorgang - ein Algorithmus - in konkrete Technik umgesetzt. Ihre Wirksamkeit beruht darauf, dass potenzielle AngreiferInnen ein gewisses mathematisches Problem nicht zu lösen vermögen - und zwar nicht wegen mangelnder Fähigkeiten, sondern wegen fehlenden Wissens um ganz bestimmte „Schlüssel“-Informationen.

Kryptographische Methoden beziehen sich stets auf folgende Situation: Ein Sender A (dieser wird, wie in der Kryptographie üblich, „Alice“ genannt) schickt über einen unsicheren Kanal eine Nachricht an einen Empfänger B (er wird „Bob“ genannt). Sender und Empfänger dürfen dabei auch identisch sein, unter einem Kanal ist ein beliebiges Transportmedium zu verstehen. Bei der Verschlüsselung lokaler Daten sind Sender und Empfänger natürlich identisch, unter „Kanal“ ist hier dann das Speichermedium zu verstehen.

[Quelle: BSI M 3.23]

10.2.2 Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt. In allen modernen Verschlüsselungsalgorithmen sind Klartexte, Geheimtexte und Schlüssel jeweils als Folgen von Bits gegeben.

Um praktisch einsetzbar zu sein, müssen Verschlüsselungsalgorithmen folgende Mindestanforderungen erfüllen:

- Sie sollten entzifferungsresistent sein, d. h. ohne Kenntnis des Schlüssels darf das Chiffrat nicht entschlüsselt werden können, insbesondere muss hierfür die Menge der möglichen Schlüssel „ausreichend groß“ sein, da sonst ein einfaches Ausprobieren aller Schlüssel möglich wäre,
- sie müssen einfach einzusetzen sein, und
- Ver-/Entschlüsselung müssen „schnell genug“ sein.

Die Forderung nach Entzifferungsresistenz ist immer relativ zu den aktuellen technischen und mathematischen Möglichkeiten zu betrachten. Wichtig bei der Bewertung von Verschlüsselungsalgorithmen ist, dass es zum Nutzungszeitpunkt praktisch nicht möglich sein darf, das Chiffrat ohne Kenntnis des Schlüssels zu entschlüsseln, d. h. nicht mit der dann verfügbaren Technik innerhalb eines akzeptablen Zeitrahmens. Wenn A und B eine vertrauliche Verbindung einrichten wollen, gehen sie wie folgt vor:

1. sie vereinbaren ein Chiffrierverfahren,
2. sie vereinbaren einen Schlüssel bzw. ein Schlüsselpaar,
3. A verschlüsselt eine Nachricht und sendet diese an B,
4. B entschlüsselt das von A gesendete Chiffrat.

Es gibt zwei große Klassen von Chiffrierverfahren:

Symmetrische Verschlüsselungsverfahren

benutzen denselben Schlüssel sowohl für die Ver- als auch für die Entschlüsselung. Symmetrische Verfahren werden deshalb gelegentlich auch als „ein-Schlüssel“-Verfahren bezeichnet, da die Kenntnis eines Schlüssels ausreicht, um chiffrieren und dechiffrieren zu können.

Bekannte symmetrische Verschlüsselungsverfahren sind z. B. DES, Tripel-DES, IDEA oder RC5.

Bei symmetrischen Verfahren unterscheidet man weiter zwischen Stromchiffren und Blockchiffren.

- Bei **Stromchiffren** wird unter Verwendung des Schlüssels eine möglichst zufällig aussehende Bitfolge (ein Bitstrom) generiert, die auf die Klarbitfolge (modulo 2) aufaddiert wird. Die Klarbitfolge wird also Bit für Bit (durch Addition von Schlüsselstrombits) verschlüsselt. Für die Sicherheit von Stromchiffren ist wesentlich, dass niemals zwei (verschiedene) Nachrichten mit demselben Schlüsselstrom verschlüsselt werden - dafür muss mit speziellen Maßnahmen (Synchronisierinformation in Form eines Spruchschlüssels) gesorgt werden.

- Bei **Blockchiffren** dagegen wird in einem Verschlüsselungstakt jeweils ein ganzer Block von Bits verschlüsselt, heutzutage sind dies in der Regel 64 Bits.

Die meisten symmetrischen Verschlüsselungsverfahren sind Blockchiffren, dazu gehören auch DES, IDEA oder RC5. Für Blockchiffren sind eine Reihe von Betriebsarten (Modi) definiert (und standardisiert). Es sind dies

- der ECB (Electronic Code Book)-Modus, bei dem jeder Block für sich - unabhängig von den anderen Blöcken - verschlüsselt wird,
- der CBC (Cipher Block Chaining)-Modus und der CFB (Cipher Feed Back)-Modus, bei denen nach Wahl eines zusätzlichen Initialisierungsvektors eine Abhängigkeit der Chiffretextblöcke von allen vorhergehenden Chiffretextblöcken hergestellt wird, sowie
- der OFB (Output Feedback Modus), der so aufgefasst werden kann, dass die verwendete Blockchiffre zur Generierung eines „Blockstroms“ verwendet wird, der auf die Klarblöcke bitweise (modulo 2) aufaddiert wird.

Beim Einsatz symmetrischer Verfahren ist generell zu beachten, dass ein Schlüsselaustausch zwischen den KommunikationspartnerInnen vorausgegangen sein muss. Dieser muss über einen sicheren Kanal (z. B. Kurier, persönliche Übergabe) erfolgen und beide Parteien müssen anschließend den Schlüssel geheim halten. Es gibt verschiedene Verfahren für einen sicheren Schlüsselaustausch.
In geschlossenen Systemen ist der Schlüsselaustausch im allgemeinen unproblematisch zu realisieren, da hier meist „sichere Kanäle“ vorhanden sind. In offenen Systemen mit einer Vielzahl von KommunikationspartnerInnen gestaltet sich dies schwieriger. Generell besteht jedoch das Problem, dass bei einer Vielzahl möglicher KommunikationspartnerInnen entsprechend viele Schlüssel vor der eigentlichen Kommunikation ausgetauscht werden müssen und dass dabei die potenziellen KommunikationspartnerInnen vorab bekannt sein müssen.

Asymmetrische Verschlüsselungsverfahren (Public-Key-Verfahren)

benutzen zwei verschiedene (aber mathematisch verwandte) Schlüssel: einen „öffentlichen“ Schlüssel (Public Key) für die Verschlüsselung, und einen „privaten“ Schlüssel (Private Key) für die Entschlüsselung. Das Schlüsselpaar muss dabei folgende Eigenschaft aufweisen: für alle, die lediglich den „Public Key“ kennen, muss es praktisch unmöglich sein, den zugehörigen „Private Key“ zu bestimmen oder eine mit dem „Public Key“ verschlüsselte Nachricht zu entschlüsseln.

Asymmetrische Verschlüsselung hat also eine „Einbahn“-Eigenschaft: eine Nachricht kann nicht wiederhergestellt werden, wenn der „Private Key“ vergessen oder gelöscht wurde.

Die Bezeichnung „Public Key“-Verschlüsselung rührt daher, dass der „Public Key“ öffentlich bekannt gemacht werden kann, ohne die Sicherheit des Verfahrens zu kompromittieren. Der „Private Key“ hingegen muss geheim gehalten werden.

Will nun Alice eine Nachricht verschlüsselt an Bob senden, so holt sich Alice den öffentlichen Schlüssel Bobs aus einer frei zugänglichen Datei und verschlüsselt damit die Nachricht. Nach Erhalt der Nachricht benutzt Bob seinen geheimen Schlüssel, um die von Alice erhaltene Nachricht zu entschlüsseln. Wenn Alice und Bob ein asymmetrisches Verfahren zum Zweck der Vertraulichkeit verwenden, benötigen sie also keinen sicheren Kanal für den Schlüsselaustausch, aber Alice muss sicher sein, dass sie tatsächlich Bobs öffentlichen Schlüssel benutzt und keinen Schlüssel, der ihr von Eve als Bobs Schlüssel untergeschoben wurde. Würde Alice eine Nachricht mit einem von Eve untergeschobenen Schlüssel verschlüsseln, so könnte Eve, der ja der passende geheime Schlüssel bekannt ist, die Nachricht entschlüsseln. Der Sender benötigt in der Regel die Bestätigung einer vertrauenswürdigen dritten Partei, dass der öffentliche Schlüssel des Empfängers wirklich zu diesem gehört. Diese Bestätigung, das „Zertifikat“, wird im allgemeinen auch durch ein kryptographisches Verfahren erzeugt und dem öffentlichen Schlüssel beigefügt.

Zwei bekannte asymmetrische Verschlüsselungsverfahren sind das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir, Adleman) und die Klasse der Elgamal-Verfahren. Zu letzteren gehören auch die auf Elliptischen Kurven basierenden Verschlüsselungsverfahren.

Vorteile (guter) symmetrischer Verfahren:

- Sie sind schnell, d. h. sie haben einen hohen Datendurchsatz.
- Die Sicherheit ist im Wesentlichen durch die Schlüssellänge festgelegt, d. h. bei guten symmetrischen Verfahren sollte es keine Attacken geben, die wesentlich besser sind als das Durchprobieren aller Schlüssel (Brute-Force-Attacken).
- Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
- Die Schlüsselerzeugung ist einfach, da gewöhnlich als Schlüssel jede Bitfolge einer festen Länge erlaubt ist und als Schlüssel eine Zufallszahl gewählt werden kann.

Nachteile symmetrischer Verfahren:

- Jeder Teilnehmer muss sämtliche Schlüssel seiner Kommunikationspartner besitzen und geheim halten.
- Zur Schlüsselverteilung sind sie weniger gut geeignet als asymmetrische Verfahren, insbesondere bei einer großen Anzahl von Kommunikationspartnern.
- Für Verbindlichkeitszwecke sind sie weniger praktikabel als asymmetrische Verfahren, da bei der Verwendung symmetrischer Schlüssel nicht ohne weiteres erkannt werden kann, welcher der beiden Kommunikationspartner die Nachricht verschlüsselt hat. Dies lässt sich nur durch eine zwischengeschaltete dritte Partei sicherstellen, die über entsprechende kryptographische Protokolle in den Nachrichtenfluss eingebunden wird.

Vorteile (guter) asymmetrischer Verfahren:

- Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.
- Sie lassen sich einfach für digitale Signaturen benutzen.
- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
- Sie sind gut geeignet für Nicht-Abstreitbarkeitszwecke.

Nachteile asymmetrischer Verfahren:

- Sie sind langsam, d. h. sie haben im allgemeinen einen geringen Datendurchsatz.
- Sicherheit: für alle bekannten Public-Key-Verfahren gilt:
    - Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden (im Vergleich zu symmetrischen Verfahren) relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
    - Die Sicherheit beruht „nur“ auf der vermuteten, aber von der Fachwelt anerkannten, algorithmischen Schwierigkeit eines mathematischen Problems (zum Beispiel die Zerlegung einer großen Zahl in die Primfaktoren).
- Die Schlüsselerzeugung ist i. Allg. komplex und aufwendig, da die Erzeugung „schwacher“ Schlüsselpaare vermieden werden muss.

Hybride Verfahren versuchen, die Vorteile beider Arten von Verschlüsselung zu kombinieren: sie benutzen asymmetrische Verschlüsselung, um einen Sitzungsschlüssel („Sessionkey“) für ein symmetrisches Verfahren zu übermitteln, und verschlüsseln die Massendaten mit dem symmetrischen Verfahren. Der Sessionkey wird gewöhnlich nur für eine Sitzung (Übertragung) verwendet und dann vernichtet. Das asymmetrische Schlüsselpaar wird je nach Umständen für einen langen Zeitraum verwendet.

[Quelle: BSI M 3.23]

10.2.3 Integritätsschutz

Das Ziel des Integritätsschutzes ist es, dass ein Empfänger einer Nachricht feststellen kann, ob er diese Nachricht unverfälscht erhalten hat. Das Grundprinzip des Integritätsschutzes besteht darin, die Nachricht unverschlüsselt und unverändert zu übersenden, gleichzeitig aber bestimmte Kontrollinformationen mitzuschicken, die die Kontrolle auf Unverfälschtheit der eigentlichen Nachricht ermöglichen. Voraussetzung dazu ist allerdings, dass der Empfänger die Kontrolldaten unmanipuliert erhält.

Für diese Kontrolldaten stellen sich damit folgende Bedingungen:

- Der Umfang der Kontrollinformationen muss möglichst gering sein, um die zusätzlich zu übertragenden Informationen zu minimieren.
- Praktisch jede Manipulation, auch nur eines einzelnen Bits der Nachricht muss anhand der Kontrollinformationen feststellbar sein.
- Die Kontrollinformationen müssen unmanipulierbar übertragen bzw. Manipulationen müssen entdeckt werden können.

Zur Berechnung der Kontrollinformationen werden typischerweise zwei Verfahren verwendet: Hashfunktionen und Message Authentication Codes.

- Eine (Einweg-)**Hashfunktion** ist eine Datentransformation mit folgenden Eigenschaften:
    - Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. Allg. kürzerer Länge abgebildet (typischerweise 128 - 160 Bit).
    - „Einweg“-Eigenschaft: Es muss „praktisch unmöglich“ sein, zu einem vorgegebenen Hashwert eine Nachricht zu finden, deren Hashwert der vorgegebene Hashwert ist.
    - Kollisionswiderstand: Es muss „praktisch unmöglich“ sein, zwei Nachrichten zu finden, die zum gleichen Hashwert führen.

  Mit Hilfe einer beiden Kommunikationspartnern bekannten Hashfunktion können A und B die Integrität einer Nachricht überprüfen: Alice hasht ihre Nachricht, und übermittelt diese und den Hashwert so an Bob, dass die Unverfälschtheit des Hashwertes gewährleistet ist. Bob hasht die empfangene Nachricht ebenfalls und vergleicht sein Ergebnis mit dem von Alice gelieferten Hashwert. Stimmen beide Werte überein, so kann er davon ausgehen, dass kein Bit der Nachricht verändert wurde.
- Ein **Message Authentication Code (MAC)** ist eine kryptographische Checksumme zur Nachrichtensicherung, also eine Datentransformation, bei der zusätzlich ein geheimer Schlüssel in die Berechnung eingeht, mit folgenden Eigenschaften:
    - Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. Allg. kürzerer Länge abgebildet.
    - Fälschungssicherheit: Für jeden, der nicht im Besitz des Schlüssels ist, muss es „praktisch unmöglich“ sein, den MAC-Wert einer neuen Nachricht zu berechnen, selbst wenn er in den Besitz einiger alter Nachrichten mit den zugehörigen MAC-Werten gelangt ist.
    - Kollisionswiderstand: Es muss „praktisch unmöglich“ sein, zwei Nachrichten zu finden, die zum gleichen MAC-Wert führen.

Besitzen Alice und Bob einen MAC und einen gemeinsamen, geheimen MAC-Schlüssel, so authentisiert Alice ihre Nachricht einfach dadurch, dass sie den MAC-Wert der Nachricht berechnet und zusammen mit der Nachricht an Bob schickt. Bob berechnet seinerseits den MAC-Wert der empfangenen Nachricht mit dem auch ihm bekannten MAC-Schlüssel. Stimmt dieser mit Alices Wert überein, so kann er davon ausgehen, dass die Nachricht authentisch ist (d. h. dass sie nicht verändert wurde und wirklich von Alice stammt). Alice hat also ihre Nachricht durch Verwendung des nur ihr und Bob bekannten Schlüssels gegenüber Bob authentisiert.MACs werden häufig auf Basis symmetrischer Chiffrierverfahren konstruiert. Die bekannteste Variante ist hierbei die Verschlüsselung einer Nachricht mit DES oder einem anderem Block-Chiffrierverfahren im CBC- oder CFB-Mode. Dabei wird als MAC der letzte verschlüsselte Block an die Nachricht angehängt. Daneben gibt es aber auch MACs, die nicht auf Chiffrierverfahren beruhen. Der MAC-Wert einer Nachricht kann als fälschungssichere, schlüsselabhängige, kryptographische Checksumme dieser Nachricht angesehen werden.

[Quelle: BSI M 3.23]

10.2.4 Authentizitätsnachweise

Bei der Authentisierung von BenutzerInnen gegenüber Kommunikationspartnern/IT-Systemen bzw. Clients gegenüber Servern sollen

- illegitime Zugriffe erkannt und abgewehrt werden,
- legitime Zugriffe erlaubt werden und
- sensible Daten auch bei Übertragungen über Netze geschützt bleiben.

Dazu sind Verfahren erforderlich, die allen Beteiligten die Feststellung der Identität ihrer KommunikationspartnerInnen unmißverständlich erlauben. Dies schließt einen Zeitaspekt ein: Alice will Bob in „real time“ davon überzeugen, dass tatsächlich sie mit ihm kommuniziert. Die Haupttechniken für solche Authentisierungen sind kryptographische Challenge-Response-Protokolle.

Hierbei sendet Bob Daten an Alice und fordert sie auf (Challenge), ihm den Besitz eines Geheimnisses (also einer Schlüsselinformation) nachzuweisen, und Alice demonstriert ihm diesen Besitz ohne das Geheimnis selbst preiszugeben, indem sie eine vom Geheimnis und seiner Challenge abhängige Antwort sendet (Response). Bob wiederum überprüft anhand der Antwort, dass zur Berechnung der Antwort wirklich das korrekte Geheimnis verwendet wurde.

Für eine „starke“ Authentisierung dürfen sich die Challenges nicht wiederholen. Bei Challenge-Response-Verfahren können sowohl symmetrische als auch asymmetrische Techniken verwendet werden.

Beispiel: Alice und Bob verständigen sich vorab auf ein symmetrisches Verschlüsselungsverfahren und einen gemeinsamen kryptographischen Schlüssel. Zur Authentisierung sendet Bob eine Zufallszahl als Challenge an Alice. Alice wiederum verschlüsselt diese Zufallszahl mit dem gemeinsamen geheimen Schlüssel und sendet das Ergebnis zurück an Bob. Im nächsten Schritt entschlüsselt Bob die Nachricht und vergleicht, ob das Ergebnis seine anfangs gewählte Zufallszahl ist. Bei Gleichheit ist es tatsächlich Alice, da nur sie den geheimen Schlüssel kennt.

[Quelle: BSI M 3.23]

10.2.5 Digitale Signaturen, elektronische Signaturen

Das kryptographische Konstrukt einer digitalen Signatur dient dem Ziel, für digitale Dateien und Nachrichten ein Pendant zur handschriftlichen Unterschrift einsetzen zu können. Dazu werden einige der schon erläuterten kryptographischen Verfahren wie Hashfunktionen und asymmetrische Verfahren zusammengeführt. Die wesentliche Voraussetzung für digitale Signaturen ist, dass jeder Teilnehmer ein nur ihm bekanntes Geheimnis besitzt, mit dem er zu beliebigen Dateien eine digitale Signatur bilden kann.

Anhand von öffentlichen Informationen ist es dann möglich, diese digitale Signatur zu überprüfen.

Man kann also eine digitale Signatur als speziellen Integritätsschutz mit zusätzlichen Besonderheiten ansehen: Sie ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Kann also anhand der öffentlich zugänglichen Informationen die digitale Signatur verifiziert werden, so ist einerseits die Integrität der signierten Datei gegeben und andererseits die Nichtabstreitbarkeit, da nur die Person, der die digitale Signatur eindeutig zugeordnet werden kann, diese Signatur anhand ihrer geheimen Informationen gebildet haben kann. Zu beachten ist, dass unterschiedliche Dateien auch unterschiedliche digitale Signaturen zur Folge haben und das geringste Änderungen an den Dateien zu nicht verifizierbaren Signaturen führen.

Beispiel: Verbreitet für digitale Signaturen ist die umgekehrte Anwendung des RSA-Verfahrens. Dabei besitzt jeder Teilnehmer einen nur ihm bekannten geheimen Signierschlüssel. Öffentlich zugänglich sind Verifizierschlüssel-Zertifikate, in denen der passende öffentliche Schlüssel und die Angaben zum Besitzer des passenden

geheimen Signierschlüssels unfälschbar miteinander verknüpft sind. Diese Zertifikate werden von vertrauenswürdigen Stellen herausgegeben, die zuvor die Personalien der Teilnehmer geprüft haben. Um für eine beliebige Datei eine digitale Signatur zu berechnen und zu prüfen, wird (von der Hard- bzw. Software) wie folgt vorgegangen:

1. A berechnet den Hashwert der ausgewählten Datei.
2. A verschlüsselt diesen Hashwert mit dem nur ihm bekannten geheimen Signierschlüssel. Das Ergebnis ist die digitale Signatur von A zu dieser Datei.
3. A überträgt die digitale Signatur gemeinsam mit dem Verifizierschlüssel-Zertifikat und der Datei an B.
4. B verifiziert das Zertifikat (z. B. mit dem öffentlichen Schlüssel einer Zertifizierungsstelle).
5. B berechnet den Hashwert der erhaltenen Datei.
6. Anhand des im Verifizierschlüssel-Zertifikat enthaltenen öffentlichen Verifizierschlüssels entschlüsselt B die digitale Signatur.
7. B vergleicht den in 4. berechneten Hashwert und die entschlüsselte Signatur. Sind sie identisch, so ist die digitale Signatur verifiziert. Besteht keine Gleichheit, kann B keine weiteren Schlüsse ziehen.
8. Nach der Verifikation der digitalen Signatur kann B als Ergebnisse festhalten:
    - Falls sichergestellt ist, dass tatsächlich nur A den geheimen Schlüssel besitzt, kann B sicher sein, dass die digitale Signatur von A, die im Verifizierschlüssel-Zertifikat aufgeführt ist, erzeugt wurde.
    - Die erhaltene Datei ist identisch mit der Datei, für die A die digitale Signatur berechnet hat.

Betont sei, dass digitale Signaturen ausschließlich die Ziele Integrität und Nichtabstreitbarkeit sicherstellen, jedoch in keiner Weise die Vertraulichkeit. Eine digital signierte Nachricht wird im Klartext übertragen, ist sie vertraulich, muss sie zusätzlich verschlüsselt werden.

Enthält eine digital signierte Datei eine Willenserklärung des Signierers, kann dann anhand der Signatur diese Willenserklärung unabstreitbar dem Signierer, ggf. auch vor Gericht, zugerechnet werden.

Die verwendeten Verifizierschlüssel-Zertifikate wiederum sind selbst von der vertrauenswürdigen Stelle digital signierte Dateien, die analog überprüft werden können und die Auskunft geben über den Verifizierschlüssel und die Person, die den dazu passenden geheimen Signierschlüssel besitzt.

Unterschiede zwischen MACs und digitalen Signaturen:

- Die digitale Signatur kann durch jeden, der das Verifizierschlüssel-Zertifikat besitzt, verifiziert werden, MACs dagegen nur durch die Parteien, die den geheimen Authentisierungsschlüssel kennen.

- Alices digitale Signatur einer Nachricht kann nur von Alice erstellt werden, der MAC-Wert einer Nachricht dagegen von beiden Parteien, Alice und Bob (und allen anderen, die den geheimen Authentisierungsschlüssel kennen). Es ist deshalb unmöglich, MACs für den Zweck der Verbindlichkeit einzusetzen.

Rechtsrahmen in Österreich:

In Österreich wird im Rechtsrahmen von „elektronischen Signaturen“ gesprochen. Es sind - je nach Einsatzgebiet - verschiedene Kategorien elektronischer Signaturen vorgesehen, vor allem:

- Qualifizierte Signatur: diese ersetzt die Schriftform und benötigt besonders sichere Technik (sog. „Qualifizierte Signaturerstellungseinheiten“ wie z. B. Chipkarten oder Hardware Security Modules) und einmalige persönliche Identifizierung. Die Sicherheit der verwendeten technischen Komponenten und Verfahren muss von einer Bestätigungsstelle - wie A-SIT - bescheinigt sein. Damit ist sichergestellt, dass die Sicherheitsauflagen des Signatur- und Vertrauensdienstegesetzes und der zugehörigen Verordnung nachweislich erfüllt sind.
- Amtssignatur: Sonderform der elektronischen Signatur, die von Behörden auf elektronischen Dokumenten (z. B. Bescheiden, Urkunden) angebracht wird.

Je höher die Qualitätsstufe, desto höher ist die Akzeptanz bzw. es entstehen besondere Rechtsfolgen, bei allerdings ebenso höheren Ansprüchen an die einzusetzenden Mittel und die Identifikation der jeweilig signierenden Person.

Siehe dazu:

- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)
- sowie die zugehörige Signatur- und Vertrauensdiensteverordnung – SVV

Überprüfung elektronischer Signaturen

Dazu benötigt der Empfänger den öffentlichen Signaturschlüssel des Signators. Einer elektronischen Signatur wird gewöhnlich ein Zertifikat des Signators beigefügt. Dieses Zertifikat ist eine elektronische Bescheinigung, mit dessen Hilfe die Zugehörigkeit des öffentlichen Signaturschlüssels zu einer Person (dem Signator) überprüft werden kann. Zertifikate werden von sogenannten Vertrauensdiensteanbietern (VDA) ausgestellt.

[Quelle: BSI M 3.23]

11 Physische und umgebungsbezogene Sicherheit

Die in diesem Abschnitt beschriebenen Maßnahmen dienen dem Schutz von Informationssystemen mittels baulichen und infrastrukturellen Vorkehrungen. Dabei sind verschiedene Schutzebenen zu betrachten, wie etwa Grundstücke, Gebäude oder Räume (Büros, Serverräume, Datenträgerarchiv, Räume für technische Infrastruktur, …).

Die nachfolgenden Fragen können bei der Beurteilung der baulichen und infrastrukturellen Sicherheit hilfreich sein:

- Lage des Gebäudes: Befindet es sich auf einem eigenen gesicherten Grundstück? Wie sind die benachbarten öffentlichen Verkehrsflächen beschaffen?
- Steht das Gebäude der betreffenden Organisation zur Alleinbenutzung zur Verfügung oder gibt es andere Mitbenutzer; wenn ja, welche?
- Wer hat Zutritt zum Gebäude?
- Gibt es eine physische Zutrittskontrolle? Ist ein Portierdienst eingerichtet?
- Stärke und Schutz/Überwachung von Wänden, Türen, Fenstern, Lüftungsschächten etc.
- Infrastruktur (Wasser-, Stromversorgung, Kommunikationsverbindungen, Klimaanlage, USV, …)
- Welche Bereiche des Grundstückes bzw. des Gebäudes sind sicherheitsrelevant?

Im Folgenden werden eine Reihe von grundlegenden Sicherheitsmaßnahmen angeführt. Welche davon in einem konkreten Fall zum Einsatz kommen, ist abhängig von Größe und Schutzbedarf der Organisation. Nach Möglichkeit sollten bauliche und infrastrukturelle Maßnahmen bereits in der Planungs- bzw. Bauphase Berücksichtigung finden, ein nachträglicher Einbau ist meist teuer oder gar unmöglich.

Weiters ist zu beachten, dass die Bedingungen bzw. Auflagen von etwaigen Versicherungen eingehalten werden.

Wo sinnvoll bzw. hilfreich werden in den nachfolgenden Maßnahmenbeschreibungen Normen beispielhaft herausgegriffen und angeführt. Dabei handelt es sich nicht um eine vollständige Aufzählung aller für einen Bereich relevanten Normen und auch nicht um verbindliche Einsatzempfehlungen, die angeführten Beispiele sollen lediglich einen Hinweis auf existierende, möglicherweise zur Anwendung kommende Normen geben und ein detailliertes Einarbeiten in die Materie erleichtern.

11.1 Bauliche und infrastrukturelle Maßnahmen

11.1.1 Geeignete Standortauswahl

Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen. Gebäude, die direkt an Hauptverkehrstrassen (Autobahn, Bundesstraße, Bahn, …) liegen, können durch Unfälle beschädigt werden, für Gebäude in Einflugschneisen von Flughäfen besteht Gefahr durch einen eventuellen Flugzeugabsturz.
- Die Nähe zu optimalen Verkehrswegen wird in vielen Fällen als Vorteil angesehen werden, kann aber - da diese Verkehrswege auch potenzielle Fluchtwege darstellen können - unter Umständen auch die Durchführung eines Anschlages erleichtern. Vor- und Nachteile sind entsprechend abzuwägen.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- Bei Überbauten von U-, S- oder Eisenbahnen kann es zu Störungen von Datenleitungen und CRT-Bildschirmen (Cathode Ray Tube) kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z. B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.
- Streunende Haustiere können Fehlalarme von Bewegungsmeldern verursachen und Personen gefährden.

11.1.2 Anordnung schützenswerter Gebäudeteile

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.

- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen.

Besteht die Möglichkeit, auch das Umfeld des Gebäudes in das Sicherheitskonzept einzubeziehen (etwa bei einer eigenen, ausschließlich der betreffenden Organisation gehörigen Liegenschaft), so können zusätzliche bauliche und technische Sicherheitsmaßnahmen getroffen werden („Perimeterschutz“, „Freilandschutz“). Dazu zählen etwa:

- Zäune und Mauern
- Tore, Schranken und Fahrzeugsperren
- Kameraüberwachung und Bewegungsmelder

11.1.3 Einbruchsschutz

> *Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden.*

Dazu gehören:

- Sicherungen bei einstiegsgefährdeten Türen oder Fenstern,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nichtbenutzten Nebeneingängen,
- einbruchgesicherte Notausgänge,
- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Den MitarbeiterInnen ist durch Regelungen bekannt zu geben, welche Maßnahmen zum Einbruchsschutz beachtet werden müssen.

In C.1 Wichtige Normen sind relevante ÖNORMEN zum Einbruchsschutz angeführt.

11.1.4 Zutrittskontrolle

Die Überwachung des Zutritts zu Gebäuden, Rechenzentren und sicherheitssensiblen Geräten zählt zu den wichtigsten physischen Schutzmaßnahmen. Ein Zutrittskontrollsystem vereinigt verschiedene bauliche, organisatorische und personelle Maßnahmen.

Das Zutrittskontrollkonzept legt die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz fest. Dazu gehören:

- Festlegung der Sicherheitszonen:
  Zu schützende Bereiche können etwa Grundstücke, Gebäude, Rechnerräume, Räume mit Peripheriegeräten (Drucker, …), Archive, Kommunikationseinrichtungen und die Haustechnik sein. Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.
- Generelle Festlegung der Zutrittskontrollpolitik:
  Hier wird grundsätzlich festgelegt, welche Personengruppen (etwa RZ-MitarbeiterInnen, OperatorInnen, FachabteilungsmitarbeiterInnen, KundInnen, Angehörige von Lieferfirmen etc.) Zutritt zu welchen Bereichen benötigen. Um die Zahl der zutrittsberechtigten Personen zu einem Raum möglichst gering zu halten, sollte auch beim IT-Einsatz der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert beispielsweise eine getrennte Lagerung von Ersatzteilen für IT-Systeme und Datenträgern den unerlaubten Zugriff von WartungstechnikerInnen auf die Datenträger.
- Bestimmung einer/eines Verantwortlichen für Zutrittskontrolle:
  Diese/r vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den in der Sicherheitspolitik festgelegten Grundsätzen.
- Dokumentation der Vergabe und Rücknahme von Zutrittsberechtigungen
- Definition von Zeitabhängigkeiten:
  Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit oder befristeter Zutritt bis zu einem fixierten Datum.
- Festlegung der Zutrittskontrollmedien:
  Es ist festzulegen, ob die Identifikation bzw. die Authentisierung durch Überwachungspersonal (persönlich oder mittels Überwachungskameras) oder durch automatische Identifikations- und Authentisierungssysteme wie Zugangscodes (Passwörter, PINs), Karten oder biometrische Methoden erfolgen soll.
- Festlegung der Rechteprüfung:
  Im Zutrittskontrollkonzept ist festzulegen, wo, zu welchen Zeiten und unter welchen Randbedingungen eine Rechteprüfung erfolgen muss, sowie welche Aktionen bei versuchtem unerlaubten Zutritt zu setzen sind.
- Festlegung der Beweissicherung:

Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre der/des Einzelnen.

- Behandlung von Ausnahmesituationen:
  Es ist u. a. sicherzustellen, dass im Brandfall die MitarbeiterInnen schnellstmöglich die gefährdeten Zonen verlassen können.

Weiters sind folgende Fragen zu klären:

- Sind beim Betreten oder Verlassen eines geschützten Bereiches Vereinzelungsmechanismen (Drehtüren, Schleusen, …) notwendig?
- Welche Maßnahmen sind bei unautorisierten Zutrittsversuchen zu setzen?
- Ist eine Nullsummenprüfung (Anmerkung - Nullsummenprüfung: Feststellung der Anzahl der im geschützten Bereich befindlichen Personen durch Vergleich der Zu- und Abgänge. Voraussetzung für eine Nullsummenprüfung ist die Installation von Vereinzelungsmechanismen) erforderlich?
- Ist das Auslösen eines „stillen Alarms“ vorzusehen? Durch Eingabe einer vereinbarten Kennung, etwa einer zusätzlichen Ziffer zur üblichen PIN, wird ein Alarm an einer entfernten Überwachungsstelle (Portier, Polizei) ausgelöst. Eine solche Maßnahme bietet Schutz gegen jemanden, der den Zugang zu geschützten Bereichen gewaltsam erzwingen will.
- Sperrmöglichkeiten bei Verlust oder Duplizierung des Zutrittskontrollmediums (Schlüssel, Karte, …) und bei Austritt von MitarbeiterInnen.
- Stehen die Kosten für die Installation, den laufenden Betrieb, die Wartung und die regelmäßige Revision des Zutrittskontrollsystems in vertretbarer Relation zum möglichen Sicherheitsrisiko?
- Ist die Kapazität des Zutrittskontrollsystems der Größe der Organisation angepasst? Insbesondere ist eine ausreichende Zahl von Kontrollstellen und eventuellen Vereinzelungsmechanismen vorzusehen, um Warteschlangen auch zu Stoßzeiten (Arbeitsbeginn, …) zu vermeiden.

Das Zutrittskontrollkonzept sollte bereits vor der Systemauswahl so detailliert wie möglich feststehen und weitgehend stabil bleiben. Überarbeitungen werden jedoch notwendig, bei

- Feststellung von Sicherheitsmängeln
- Erweiterungen des sicherheitsrelevanten Bereiches
- schlechter Benutzerakzeptanz:
  Die Akzeptanz durch die BenutzerInnen ist ein entscheidendes Kriterium. Mängel im Zutrittskontrollsystem (häufige Fehlalarme, Ausfälle, Wartezeiten, zu restriktive Handhabung, überflüssige bürokratische Abläufe) können dazu führen, dass auch grundsätzlich sicherheitsbewusste Mitarbeiter bereit sind, die Regeln zu verletzen.

Für Zutrittskontrollsysteme, bei denen keine biometrischen Daten von Betroffenen verarbeitet werden, ist keine Datenschutz-Folgenabschätzung notwendig, da diese in den Ausnahmen der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) aufgeführt sind. Die Verarbeitung biometrischer Daten von Betroffenen erfordert zwingend eine Datenschutz-Folgenabschätzung, sofern die Verarbeitung nicht die bloße Echtzeitwiedergabe von Gesichtsbildern betrifft (siehe Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, DSFA-V § 2 Abs. 2 Z 4).

11.1.5 Verwaltung von Zutrittskontrollmedien

Für alle Schlüssel eines Gebäudes ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren.

Zu beachten ist:

- Ist eine Schließanlage vorhanden, so sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden, ggf. einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt gegen Quittung und ist zu dokumentieren.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Bei Zuständigkeitsänderungen von MitarbeiterInnen sind deren Schließberechtigungen zu prüfen und Schlüssel gegebenenfalls einzuziehen.
- Beim Ausscheiden von MitarbeiterInnen sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel).
- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf getauscht werden, um so illegal nachgefertigten Schlüsseln die Funktion zu nehmen.
- Abhängig von der Sensibilität des zu schützenden Bereiches können auch gesperrte Schließsysteme zum Einsatz kommen, die die Anfertigung eines Schlüssels nur unter Vorliegen definierter Bedingungen (etwa schriftliche Zustimmung einer/eines Verantwortlichen) erlauben.

Das Gleiche gilt sinngemäß auch für alle anderen Zutrittskontrollmedien wie Magnetstreifen-, Chipkarten bzw. so genannte Multifunktionschipkarten.

11.1.6 Portierdienst

Die Einrichtung eines Portierdienstes hat weit reichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen.

Voraussetzung ist allerdings, dass bei der Durchführung des Portierdienstes einige Grundprinzipien beachtet werden.

- Der Portier beobachtet bzw. kontrolliert alle Personenbewegungen am Eingang zum Gebäude bzw. sicherheitsrelevanten Bereich.
- Unbekannte Personen haben sich beim Portier zu legitimieren.
- Der Portier hält vor Einlassgewährung von BesucherInnen bei den Besuchten Rückfrage.
- Die BesucherInnen werden zu den Besuchten begleitet oder am Eingang abgeholt.
- Dem Portier müssen die MitarbeiterInnen bekannt sein. Scheiden MitarbeiterInnen aus, ist auch der Portier zu unterrichten, ab wann diesen MitarbeiterInnen der Einlass zu verwehren ist.
- Abhängig von der Sensibilität des Bereiches sind die Führung eines Besucherbuches, in dem der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden kann, sowie die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen zu erwägen.

Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Portier im Zusammenspiel mit weiteren Schutzmaßnahmen zukommen (z. B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

11.1.7 Einrichtung einer Postübernahmestelle

Die Übernahme von Briefen und Paketen sollte durch eine zentrale Stelle unter Beachtung von für die betreffende Organisation adäquaten Sicherheitsregeln erfolgen.

Solche Regeln können etwa sein:

- Pakete, die von einem Botendienst o.ä. gebracht werden, dürfen erst nach Rücksprache mit den namentlich angeführten EmpfängerInnen oder berechtigten VertreterInnen übernommen werden.
- Pakete, die ohne namentlich angeführte EmpfängerInnen an die Organisation adressiert sind und von einem Paket- oder Botendienst bzw. von einer Privatperson gebracht werden, sind nicht zu übernehmen.

- Wird außerhalb der Amts- bzw. Bürostunden ein Brief oder ein Paket abgegeben, so ist von der Dienst habenden Mitarbeiterin bzw. vom Dienst habenden Mitarbeiter (z. B. Portier, Operator, …) bei den EmpfängerInnen rückzufragen, ob eine Sendung erwartet wird. Ist dies nicht der Fall oder sind die EmpfängerInnen nicht erreichbar, so ist die Sendung nicht anzunehmen.
- Für größere Organisationseinheiten ist die Beschaffung von Geräten zum Durchleuchten von Postsendungen zu erwägen.

11.1.8 Perimeterschutz

Sofern es die Gegebenheiten und die Infrastruktur zulassen, sollten bereits auf dem Grundstück der Organisation zusätzliche Sicherheitseinrichtungen installiert werden, um äußeren Gefährdungen entgegenzuwirken.

Je nach Art und Topologie der Infrastruktur bzw. des Grundstückes können folgende Vorkehrungen sinnvoll sein:

- Einfriedung des Grundstückes
  z. B. Zaunanlage, Schutzmauer
- Freiland Sicherungsmaßnahmen
  z. B. entsprechende Geländegestaltung, geeignete Beleuchtung, Detektionssensorik, Schutz durch Bewachungsunternehmen
- äußere Zutrittskontrollmechanismen
  z. B. Videoüberwachung, Personen- oder Fahrzeugschleusen

Entscheidend ist, dass der Perimeterschutz in ein stimmiges Gesamtschutzkonzept eingebettet ist, in dem die Verhältnismäßigkeiten der einzelnen Schutzmaßnahmen aufeinander abgestimmt sind.

11.2 Brandschutz

Brandschutz stellt die Gesamtheit aller Maßnahmen dar, die die Entstehung und Ausbreitung von Bränden verhindern und die Bekämpfung von Bränden gewährleisten.

Grundsätzlich ist davon auszugehen, dass die ArbeitgeberInnen und ArbeitnehmerInnen alle Maßnahmen zu ergreifen haben, um das Risiko einer Brandentstehung zu minimieren.

11.2.1 Einhaltung von Brandschutzvorschriften und Auflagen

Die gesetzlichen Brandschutzvorschriften und die Auflagen der zuständigen Baubehörde sowie der örtlichen Feuerwehr sind unbedingt einzuhalten.

Brandverhütungsstellen oder BrandschutzexpertInnen können und sollen bei der Brandschutzplanung hinzugezogen werden.

In C.1 Wichtige Normen sind eine Reihe von wichtigen Normen zum Thema Brandschutz angeführt.

Ebenso ist es notwendig, die allgemeinen und speziellen Bestimmungen des Arbeitnehmerschutzes und die Arbeitsstättenverordnung bei der Errichtung und beim Betrieb zu beachten, insbesondere

- Bundes-Bedienstetenschutzgesetz
- ArbeitnehmerInnenschutzgesetz

und die dazu ergangenen Verordnungen.

Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen des Verbands der Schadensversicherer (VdS) in Deutschland zu finden sind (Adresse siehe F Wichtige Adressen).

11.2.2 Raumbelegung unter Berücksichtigung von Brandlasten

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge, Gardinen und dergleichen.

Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im selben Raum und in den benachbarten Räumen erfolgen. So sollte etwa das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager oder Räumen mit erhöhter Brandlast untergebracht sein.

11.2.3 Organisation Brandschutz

Brandschutz umfasst sowohl präventive Maßnahmen, die die Möglichkeit einer Brandentstehung minimieren sollen, als auch Maßnahmen zur Brandbekämpfung und Evakuierung.

Präventive Maßnahmen
können sowohl technischer (z. B. Ersatz leicht entzündlicher Arbeitsstoffe) als auch organisatorischer Natur sein.

Organisatorische Maßnahmen

umfassen personenbezogene Unterweisungen (keine Zigaretten in den Papierkorb, keine Verwendung von Heizstrahlern, Ausschalten von Kaffeemaschinen bei Dienstende, …) sowie die Erstellung einer Brandschutzordnung.

Die Brandschutzordnung ist im Falle von erhöhtem Brandschutz zu erstellen und umfasst die zur Brandverhütung erforderlichen technischen und organisatorischen Vorkehrungen und Maßnahmen. Sie ist allen Bediensteten *jährlich einmal nachweislich* zur Kenntnis zu bringen.

Maßnahmen zur Brandbekämpfung und Evakuierung beinhalten u. a.

- die Bestellung von Brandschutzbeauftragten,
- die Unterweisung der ArbeitnehmerInnen über die Verwendung der Feuerlöscheinrichtungen,
- die Ausarbeitung eines Evakuierungsplanes und
- regelmäßige Brandschutzübungen

11.2.4 Brandabschottung von Trassen

Bei Gebäuden mit mehreren Brandabschnitten lässt es sich kaum vermeiden, dass Trassen durch Brandwände und Decken führen. Die Durchbrüche sind nach Verlegung der Leitungen entsprechend dem Brandwiderstandswert der Wand bzw. Decke zu schotten (wieder zu verschließen). Um die Nachinstallation zu erleichtern, können geeignete Materialien verwendet werden. Entsprechende Richtlinien und Normen (etwa ÖNORM B 3836 und B 3850, siehe A.1 Sicherheitsszenarien) sind dabei zu beachten.

Brandabschottungen sind bautechnische Maßnahmen, die einen Durchbruch durch einen Brandabschnitt über eine bestimmte Zeitdauer gegen Durchtritt eines Brandes abdichten (z. B. bei Leitungs- oder Kabeldurchführungen).

Es sind hier verschiedene Systeme wie z. B. Brandschutzziegel, Brandschutzkissen oder Spachtelmassen am Markt. Wichtig ist neben einer Zulassung des Systems auch eine genaue Einhaltung der Verarbeitungsanleitungen.

Die Nichtabschottung von nachträglichen Verkabelungen ist ein immer wieder anzutreffender Schwachpunkt im baulichen Brandschutz.

Die angeführten Themenbereiche finden u. a. in den jeweiligen Bauordnungen der Länder, den Arbeitnehmerschutzvorschriften und in den behördlichen Vorschreibungen und Genehmigungen ihren Niederschlag.

Bei der Trassenplanung sollte die für den Brandschutz verantwortliche Person hinzugezogen werden.

11.2.5 Verwendung von Brandschutztüren und Sicherheitstüren

Brandschutztüren sind Brandschutzabschlüsse, welche hinsichtlich ihrer Brandwiderstandsdauer der ÖNORM B 3850 entsprechen müssen.

Im Regelfall ist bei der Bildung eines Brandabschnittes bezüglich der Tür eine geringere Brandwiderstandsklasse gefordert als bei der Brandwand (meistens REI 90 für Wände und EI2 30-C für Türen).

Brandschutztüren auf Verkehrswegen sind bei Vorhandensein einer Brandmeldeanlage an diese anzuschließen, um ein Aufkeilen zu verhindern. Ansonsten sollten bei solchen Türen Feststellanlagen mit oder ohne eigene Branderkennung (Brandmelder) installiert werden.

Sicherheitstüren, wie z. B. Stahlblechtüren, bieten gegenüber normalen Bürotüren Vorteile:

- Sicherheitstüren (einbruchhemmende Türen) bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Keller- und Lieferanteneingängen).
- Brandschutztüren verzögern die Ausbreitung eines Brandes.

Wichtige ÖNORMEN dazu werden in C.1 Wichtige Normen angeführt.

Der Einsatz von Sicherheitstüren ist über den von der Feuerwehr vorgeschriebenen Bereich hinaus (vgl. 11.2.1 Einhaltung von Brandschutzvorschriften und Auflagen) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv vorzusehen.

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit Anschluss an die Brandmeldeanlage und einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

11.2.6 Brandmeldeanlagen

Brandmeldeanlagen (BMA) dienen zur Überwachung eines bestimmten, besonders gefährdeten Bereiches oder eines gesamten Gebäudes. Derartige Brandmeldeanlagen können mit einer TUS-Leitung (Tonfrequentes Übertragungssystem) direkt mit der Feuerwehr verbunden sein oder intern auf einer kompetenten, ständig besetzten Stelle auflaufen.

Entsprechend den Anschlussbedingungen müssen alle neuen Brandmeldeanlagen über eine Interventionsschaltung verfügen, was bedeutet, dass nach dem ersten Brandalarm 3 bis 6 Minuten Zeit verbleiben um die Meldung zu überprüfen. Wird diese Brandmeldung in der vorgesehenen Zeit nicht quittiert, bzw. gelangen während der Überprüfungszeit eine oder mehrere weitere Meldungen zur Brandmeldeanlage, werden diese sofort an die Feuerwehr weitergeleitet.

Bereits in Betrieb befindliche Brandmeldeanlagen mit einem TUS-Anschluss müssen, je nach Größe des Überwachungsbereiches, umgebaut werden und eine Interventionsschaltung aufweisen.

Derartige Anlagen werden von der Behörde vorgeschrieben und sind nach der TRVB S 123 (Brandmeldeanlagen) und TRVB S 114 (Anschaltebedingungen von Brandmeldeanlagen an öffentliche Feuerwehren) zu errichten. Sie sind jährlich durch eine Wartungsfirma und alle 2 Jahre durch eine autorisierte Prüfstelle zu überprüfen.

11.2.7 Brandmelder

Brandmelder dienen zur Früherkennung von Brandgefahren und werden in automatische und nichtautomatische Melder unterschieden, welche an einer Brandmeldeanlage hängen oder als Einzelmelder fungieren.

Bei *automatischen Brandmeldern* unterscheidet man:

- Ionisationsrauchmelder
  Bei Ionisationsrauchmeldern erfolgt die Branderkennung durch die Änderung des Stromflusses in der Ionisationskammer. Dieser Stromfluss wird durch Ionisation der Luft in der Messkammer erzeugt. Dringen nun Rauchpartikel, welche Träger der ionisierten Luftmoleküle sind, in die Kammer ein, ändert sich der Stromfluss.
- Streulichtmelder
  Die Erkennungsgröße ist bei diesem Melder die Streuung eines definierten Lichtstrahles durch eindringenden Rauch.
- Wärmemelder (Maximal- oder Differentialmelder)
  Als Kriterium wird entweder eine definierte Maximaltemperatur bzw. ein Temperaturanstieg herangezogen.
- Flammenmelder
  Bei Flammenmeldern erfolgt die Branderkennung durch die von Bränden ausgehende Strahlung. Sie können auch bei starken Luftbewegungen eingesetzt werden und haben eine große Überwachungsfläche.

Nichtautomatische Brandmelder:

- Druckknopfmelder
  Durch Drücken des Melders wird die Brandmeldung über die Brandmeldeanlage direkt - ohne Verzögerung - an die Feuerwehr weitergeleitet.

Bei der Auswahl der Brandmelder sind folgende Kriterien zu beachten

- Art des Brandverlaufes
- Rauchentwicklung
- Rascher Temperaturanstieg
- Täuschungsanfälligkeit (z. B. Teeküchen - Aerosolbildung)
- Raumhöhen
- Überwachungsflächen

11.2.8 Handfeuerlöscher (Mittel der Ersten und Erweiterten Löschhilfe)

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn entsprechende Handfeuerlöscher in der jeweils geeigneten Brandklasse (ÖNORM EN 2:1993 02 01) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben.

Pulverlöscher mit Eignung für Brandklasse E bis 1000 V sind für elektrisch betriebene Peripheriegeräte geeignet, für elektronisch gesteuerte Geräte, z. B. Rechner, sollten Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen.

Dabei ist zu beachten:

- Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden.
- Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind.
- Die Beschäftigten haben sich über die Standorte der nächsten Feuerlöscher zu informieren.
- Bei entsprechenden Brandschutzübungen sind die MitarbeiterInnen in der Handhabung der Handfeuerlöscher zu unterweisen.

11.2.9 Löschanlagen

Löschanlagen der verschiedensten Ausführungen sind meistens mit einer Brandmeldeanlage gekoppelt und werden im Bedarfsfall von dieser selbstständig ausgelöst. Diese werden meistens von der Behörde bei Vorlage einer erhöhten Brandgefährdung vorgeschrieben, um Entstehungsbrände effizient zu bekämpfen bzw. eine Ausbreitung zu unterbinden.

Sprinkleranlagen
Sprinkleranlagen sind automatisch wirkende Löschanlagen mit dem Löschmittel Wasser. Die Auslösung der Anlage erfolgt durch thermische Zerstörung der Sprinklerkopfabschlüsse (im Normalfall alkoholgefüllte Glasviolen). Dadurch wird der Austritt von Wasser durch den Sprinklerkopf freigegeben.

Bei der Auslegung der Anlage (Löschwasserleistung, Wirkfläche und Löschwasserbevorratung) ist die Brandbelastung des jeweils betroffenen Bereiches zu berücksichtigen.

CO2-Löschanlagen
CO2-Löschanlagen sind Gaslöschanlagen mit dem Löschmittel CO2. Bei der Planung ist neben der brandschutztechnisch richtigen Auslegung die erstickende Wirkung des CO2 als wesentlicher Faktor zu berücksichtigen. Es muss daher nach Branderkennung eine sofortige Alarmierung der betroffenen Personen und eine Schließung des Flutungsbereiches erfolgen. Die Einleitung des CO2 darf erst nach ausreichender Verzögerung zum Zwecke des Verlassens des Bereiches erfolgen. Die Auslösung des Löschmittels muss händisch unterbrechbar sein.

(ehemals) Halonlöschanlagen
Seit 2004 gilt in der EU ein Verbot von Halon betriebenen Löschgeräten (FCKW, welches die Ozonschicht zerstört). Als Ersatz werden natürliche oder chemische Löschmittel sowie Sprinkleranlagen verwendet.

Schaumlöschanlagen
Schaumlöschanlagen sind Löschanlagen mit dem Löschmittel Schaum, welche ähnlich wie Sprinkleranlagen funktionieren.

11.2.10 Brandschutzbegehungen

Die Erfahrungen zeigen, dass im täglichen Betrieb die Vorschriften und Regelungen zum Brandschutz immer nachlässiger gehandhabt werden - oft bis hin zur völligen Ignoranz.

Einige Beispiele dazu:

- Fluchtwege werden blockiert, z. B. durch Möbel und Papiervorräte.
- Brandabschnittstüren werden durch Keile offen gehalten.
- Zulässige Brandlasten werden durch anwachsende Kabelmengen oder geänderte Nutzungen überschritten.
- Brandabschottungen werden bei Arbeiten beschädigt und nicht ordnungsgemäß wiederhergerichtet.

Aus diesem Grund sollten ein- bis zweimal im Jahr Brandschutzbegehungen - angekündigt oder unangekündigt - erfolgen. Vorgefundene Missstände müssen dazu Anlass geben, die Zustände und deren Ursachen unverzüglich zu beheben.

Im Wiederholungsfall oder bei besonders eklatanten Verstößen gegen die Brandschutzvorschriften sind auch entsprechende Sanktionen vorzusehen.

11.2.11 Rauchverbot

In Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Die Einhaltung des Rauchverbotes ist zu kontrollieren.

11.2.12 Rauchschutzvorkehrungen

Im Brandfall geht von der damit verbundenen Rauchentwicklung sowohl für Mensch als auch für IT-Gerätschaften eine erhebliche Gefahr aus. Ein umfassender Rauchschutz ist daher vorzusehen.

In diesem Sinne ist zu gewährleisten, dass

- rauchdichte Brandschutztüren verwendet werden (vgl. 11.2 Brandschutz),
- Rauchschutztüren verwendet werden, die ggf. bei Rauchentwicklung selbsttätig geschlossen werden und die Rauchausbreitung verhindern,
- die Lüftungsanlage eine Ablüftung von Rauch vornehmen kann und
- die Lüftungs- und Klimaanlage selbsttätig auf Rauchentwicklung reagiert.

11.3 Stromversorgung, Maßnahmen gegen elektrische und elektromagnetische Risiken

11.3.1 Angepasste Aufteilung der Stromkreise

Die Raumbelegung und die Anschlusswerte, für die eine Elektroinstallation ausgelegt wurde, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimaanlage, Beleuchtung etc.) die Elektroinstallation zu prüfen und ggf. anzupassen. Das kann durch Umrangierung von Leitungen geschehen. Andernfalls kann die Neuinstallation von Einspeisung, Leitungen, Verteilern etc. erforderlich werden.

11.3.2 Not-Aus-Schalter

Bei Räumen, in denen elektrische Geräte in der Weise betrieben werden, dass z. B. durch deren Abwärme, durch hohe Gerätedichte oder durch Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist nach Möglichkeit die Installation eines Not-Aus-Schalters vorzusehen. Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

Zu beachten ist, dass lokale unterbrechungsfreie Stromversorgungen (USV) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird (siehe auch 11.3.4 Lokale unterbrechungsfreie Stromversorgung).

Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (evtl. mit Lagehinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden. Dabei ist allerdings zu bedenken, dass dieser Not-Aus-Schalter auch unnotwendigerweise versehentlich oder absichtlich betätigt werden kann.

11.3.3 Zentrale Notstromversorgung

In Bereichen, in denen die Stromversorgung bei Ausfällen des öffentlichen Netzes über einen längeren Zeitraum aufrechtzuerhalten ist - dies kann sowohl für die Versorgung von IT-Anlagen als auch der Infrastruktur gelten - ist eine zentrale Notstromversorgung vorzusehen.

Diese wird in der Regel als Diesel-Notstrom-Aggregat realisiert. In einzelnen Fällen, wo die Verfügbarkeitsanforderungen es zulassen, kann die Notstromversorgung auch in Form einer zweiten Energieeinspeisung aus dem Netz eines zweiten Energieversorgungsunternehmens (EVU) realisiert werden.

11.3.4 Lokale unterbrechungsfreie Stromversorgung

Mit einer unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, dass ein geordnetes Herunterfahren angeschlossener Rechner möglich ist.

Dies ist insbesondere dann sinnvoll, wenn

- im Rechner umfangreiche Daten zwischengespeichert werden (z. B. Cache-Speicher im Netz-Server), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
- beim Stromausfall ein großes Datenvolumen verloren gehen würde und nachträglich nochmals erfasst werden müsste,
- die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist.

Drei Arten der USV sind zu unterscheiden:

- Off-line-USV: Hierbei werden die angeschlossenen Verbraucher im Normalfall direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung.
- Netzinteraktive USV: Eine Weiterentwicklung der off-line-USV, bei der die eingehende Netzspannung über einen automatischen Spannungsregelkreis (AVR) direkt an den Verbraucher weitergeleitet wird. Wird von der USV-Elektronik ein Netzausfall erkannt, schaltet sie den bereits netzsynchron mitlaufenden Wechselrichter von Netzversorgung auf Batterieeinspeisung um.
- On-line-USV: Hier ist die USV ständig zwischen Netz und Verbraucher geschaltet. Die gesamte Stromversorgung läuft immer über die USV.

Alle 3 USV-Arten können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch (mehr oder weniger gut) dazu dienen, Überspannungen zu glätten.

Bei der Dimensionierung einer USV kann man i. d. R. von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, so dass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben, um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länger andauern. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die nach einer vorher festgelegten Zeit, entsprechend dem Zeitbedarf der IT und der Kapazität der USV, ein rechtzeitiges automatisches Herunterfahren (Shut-down) einleiten können. Für spezielle Anwendungsfälle (z. B. TK-Anlagen) kann die erforderliche Überbrückungszeit auch mehrere Stunden betragen.

Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der USV vorzusehen.

Falls die Möglichkeit besteht, die Stromversorgung unterbrechungsfrei aus einer anderen Quelle zu beziehen (z. B. durch Anschluss an eine zentrale USV), so stellt dies eine Alternative zur lokalen USV dar.

Weiters ist zu beachten:

- Die USV ist regelmäßig - entsprechend den Angaben des Herstellers - zu warten.
- Die Wirksamkeit der USV ist regelmäßig zu testen.

- Im Falle von Veränderungen ist zu überprüfen, ob die vorgehaltene Kapazität der USV noch ausreichend ist.

In diesem Zusammenhang ist auch 11.3.2 Not-Aus-Schalter zu beachten.

11.3.5 Blitzschutzeinrichtungen (Äußerer Blitzschutz)

Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u. ä.) lassen sich durch die Installation einer Blitzschutzanlage verhindern.

Über diesen „äußeren Blitzschutz“ hinaus ist fast zwingend der „innere Blitzschutz“, der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt die elektrischen Betriebsmittel im Gebäude **nicht.** Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu 11.3.6 Überspannungsschutz (Innerer Blitzschutz), dessen hohe Kosten dem Schutzgut gegenüber gerechtfertigt sein müssen).

11.3.6 Überspannungsschutz (Innerer Blitzschutz)

Je nach Qualität und Ausbau des Versorgungsnetzes des Energieversorgungsunternehmens und des eigenen Stromleitungsnetzes, abhängig vom Umfeld (andere Stromverbraucher) und von der geographischen Lage, können durch Induktion oder Blitzschlag Überspannungsspitzen im Stromversorgungsnetz entstehen.

Überspannungen durch Blitz haben i. d. R. ein recht hohes zerstörerisches Potenzial, während Überspannungen anderer Ursachen geringer sind, aber trotzdem ausreichen können, um Mikroelektronikgeräte zu stören oder zu zerstören.

Der Überspannungsschutz wird in der Regel in drei voneinander abhängigen Stufen aufgebaut:

- Grobschutz:
  Geräte für den Grobschutz vermindern Überspannungen, wie sie durch direkten Blitzschlag entstehen, und begrenzen sie auf ca. 6000V. Für die Auswahl des Grobschutzes ist es bedeutend, ob ein äußerer Blitzschutz vorhanden ist oder nicht.
- Mittelschutz:
  Der Mittelschutz begrenzt die verbleibende Überspannung auf ca. 1500 V und ist auf die Vorschaltung eines Grobschutzes angewiesen.
- Feinschutz:
  Geräte für den Feinschutz senken Überspannungen so weit herab, dass sie auch für empfindliche Bauteile mit Halbleiterbauelementen ungefährlich sind.

Weiters ist zu beachten:

- Blitz- und Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. ersetzt werden.
- Potenzialausgleich: Nur wenn alle Schutzeinrichtungen sich auf das gleiche Potenzial beziehen, ist ein optimaler Schutz möglich. Bei Nachinstallationen ist darauf zu achten, dass der Potenzialausgleich mitgeführt wird.

11.3.7 Schutz gegen elektromagnetische Einstrahlung

Die Funktion informationstechnischer Geräte kann durch die elektromagnetische Strahlung benachbarter Einrichtungen beeinträchtigt werden. Mögliche Ursachen für solche Störstrahlungen sind Radarstrahlung, Mobilfunk-, Rundfunk- und Fernsehsender, Richtfunkanlagen, Hochspannungsleitungen, Maschinen, von denen elektromagnetische Störungen ausgehen können (Schweißgeräte, Anlagen mit starken Elektromotoren, Mikrowellenherde usw.) oder atmosphärische Entladungen.

So weit möglich, sollten solche Störquellen bereits bei der Planung berücksichtigt bzw. ausgeschaltet werden. Als nachträgliche Maßnahmen bleiben etwa:

- die Verwendung von Schutzschränken mit speziellen Filtern und Türdichtungen oder
- die Abschirmung durch beschichtete Wände.

Anmerkung: Diese Maßnahme behandelt den Schutz gegen Störstrahlung im täglichen Umfeld. Schutz gegen einen elektromagnetischen Puls (EMP) als Folge kriegerischer Handlungen gehen über den mittleren Schutzbedarf hinaus und sind daher nicht Gegenstand des vorliegenden Handbuches.

11.3.8 Schutz gegen kompromittierende Abstrahlung

Überall dort, wo Information elektronisch übertragen, verarbeitet oder dargestellt wird, ist die Gefahr der kompromittierenden Abstrahlung gegeben. Bildschirme, Tastaturen, Drucker, Modems, Graphikkarten, LAN-Komponenten, Fax-Geräte und ähnliche Geräte geben elektromagnetische Wellen ab, die noch in einer Entfernung von mehreren Metern - bei Monitoren bis zu mehreren hundert Metern - aufgefangen und analysiert werden können (Side-Channel-Attacken). In der Nähe geführte Leitungen (Heizkörper, Wasserleitungen, …) können diese Abstrahlung beträchtlich verstärken.

Abwehrmaßnahmen

Möglichkeiten, den Verlust der Vertraulichkeit von Daten durch kompromittierende Abstrahlung zu verhindern, sind etwa:

- Auswahl des Standortes (innerhalb eines Gebäudes):
  Bereits eine geeignete Aufstellung von IT-Komponenten, die entsprechend vertrauliche Daten verarbeiten oder übertragen und bei denen die Gefahr einer kompromittierenden Abstrahlung besteht, kann das potenzielle Risiko durch kompromittierende Abstrahlung in erheblichem Maße verringern. Daher sollten, soweit baulich, technisch und organisatorisch möglich, potenziell gefährdete Komponenten in Räumen untergebracht werden, die möglichst weit entfernt von Straßenfronten und Gebäuden mit Fremdfirmen sind. Weiters ist eine Aufstellung in der Nähe von Leitungen (Heizungsrohre, Heizkörper, Wasserleitungen, …) zu vermeiden.
- Schirmung von Geräten:
  Diese erfolgt durch die Verwendung spezieller Materialien. Solche abstrahlsichere Hardwarekomponenten werden in Anlehnung an den englischen Fachausdruck meist als „tempest-proof“ oder „tempest-gehärtet“ bezeichnet. [Anmerkung: Für die Bedeutung des Wortes TEMPEST werden verschiedene Erklärungen genannt, z. B. „Temporary Emission and Spurious Transmission“, „Transient Electromagnetic Pulse Emanation Surveillance Technology“ oder „Transient Electromagnetic Pulse Emanations Standard“. Es wird auch die Meinung vertreten, dass es sich nicht um ein Akronym, sondern um einen Codenamen ohne besondere Bedeutung handelt.]
- Schirmung von Räumen und Gebäuden:
  Anstelle eines Schutzes auf Geräteebene ist - bei entsprechenden Gegebenheiten - auch ein Schutz auf Raum- oder Gebäudeebene möglich. Dabei werden Wände, Böden und Decken entsprechend abgeschirmt. Auch Spezialglas, das mit einem transparenten Metallfilm beschichtet ist, wird am Markt angeboten, da selbstverständlich Fenster in den Schutz mit einzubeziehen sind. Eine Raumschirmung schützt i. Allg. auch gegen Störstrahlung von außen.
- Überlagerung der kompromittierenden Abstrahlung:
  Durch Senden von Störddaten in einer bestimmten Frequenzbreite können die Emissionen der DV-Geräte überlagert werden.

Selbst bei der Verwendung von kleinsten Geräten wie beispielsweise Kryptomodulen oder Smartcards ist auf deren kompromittierende Strahlung zu achten. Gerade bei sicherheitsrelevanten Anwendungen (Zugangssystemen, kryptographische Anwendungen etc.) ist deren Schutzbedarf immens. In diesem Zusammenhang sind die Möglichkeiten von Side-Channel-Attacken (Differential Power Analysis - DPA, Differential Electro-Magnetic Analysis - DEMA) zu berücksichtigen. Demnach sind bereits bei der Anschaffung von Geräten jene mit entsprechenden Gegenmaßnahmen zu bevorzugen.

Auch das Überkoppeln auf Leitungen ist eine Auswirkung von kompromittierender elektromagnetischer Strahlung. Wird ein Signal leitungsgebunden übertragen, so ist der elektrische Leiter mit einem elektromagnetischen Feld umgeben. Dieses Feld erzeugt auf in unmittelbarer Umgebung des Leiters verlegten Kabeln Spannungen und Ströme, aus denen das Signal des ursächlichen Leiters wiedergewonnen

werden kann. Dabei spielt es keine Rolle, ob es sich um eine analoge oder digitale Nachrichtenübertragung handelt. In beiden Fällen kann mit recht einfachen Maßnahmen das ursprüngliche Signal wiederaufbereitet werden. Geeignete Schutzmaßnahmen sind:

- Wahl geeigneter Kabeltypen wie beispielsweise Koaxial- oder Twisted-Pair-Kabeln
- Achten auf hochwertige Schirmung der Kabel (vorzugsweise ist doppelte Schirmung zu verwenden - Kombination aus Folien- und Geflechtschirmung)
- Verlegung parallel geführter Kabel in ausreichendem Abstand zueinander
- Verringerung des Signal-Oberwellengehaltes durch elektrische Filterung (besonders bei digitalen Übertragungen)
- Vorzugsweise Verwendung von Lichtwellenleitern (Gefahr des Übersprechens deutlich geringer aber in Folge mechanischer Beschädigungen des Kabels ebenfalls möglich)

11.3.9 Schutz gegen elektrostatische Aufladung

Elektrostatische Aufladungen können Schäden an Bauteilen, Programmstörungen oder Datenverluste verursachen. Aus diesem Grund wird für Komponenten, die in ungeschützter Umgebung eingesetzt werden, eine relativ hohe Widerstandsfähigkeit gegen elektrostatische Aufladung gefordert.

Zieht man allerdings in Betracht, dass abhängig von Bodenbeschaffenheit - hier stellen insbesondere Teppichböden eine Gefahrenquelle dar - und Schuhwerk die elektrostatische Aufladung von gehenden Personen 10 kV und mehr betragen kann, so zeigt sich die Notwendigkeit von Maßnahmen zur Vermeidung und Eliminierung elektrostatischer Aufladungen.

Solche Maßnahmen sind etwa:

- die Gewährleistung einer relativen Luftfeuchtigkeit von mindestens 50 %,
- die Verwendung geeigneter Werkstoffe (Bodenbeläge, …),
- Erdungsmaßnahmen,
- der Einsatz von Antistatikmitteln.

11.4 Leitungsführung

11.4.1 Lagepläne der Versorgungsleitungen

Es sind genaue Lagepläne aller Versorgungsleitungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung etc.) im Gebäude und auf dem dazugehörenden Grundstück zu führen und alle die Leitungen betreffenden Sachverhalte aufzunehmen:

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- evtl. vorhandene Kennzeichnung,
- Nutzung der Leitungen (Nennung der daran angeschlossenen Netzteilnehmer, soweit möglich und zweckmäßig),
- Gefahrenpunkte und
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand der Pläne einfach und schnell ein genaues Bild der Situation zu machen. Nur so kann das Risiko, dass Leitungen bei Arbeiten versehentlich beschädigt werden, auf ein Mindestmaß reduziert werden. Eine Schadstelle ist schneller zu lokalisieren, die Störung schneller zu beheben.

Weiters ist zu beachten:

- Alle Arbeiten an Leitungen sind rechtzeitig und vollständig zu dokumentieren.
- Die Pläne sind gesichert aufzubewahren, der Zugriff darauf ist zu regeln, da sie schützenswerte Informationen beinhalten.
- Die Verantwortlichkeiten für Aktualisierung und Aufbewahrung der Pläne sind festzulegen.

Vgl. dazu auch 12.2.5 Dokumentation und Kennzeichnung der Verkabelung und 11.3.8 Schutz gegen kompromittierende Abstrahlung.

11.4.2 Materielle Sicherung von Leitungen und Verteilern

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes und zugehöriger Bereiche ist es sinnvoll, Leitungen und Verteiler zu sichern.

Dies kann auf verschiedene Weise erreicht werden, etwa:

- Verlegung der Leitungen unter Putz,
- Nagetierschutz,
- Verlegung der Leitungen in Stahl- oder Kunststoffpanzerrohren,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- bei Bedarf zusätzlich elektrische Überwachung von Verteilern und Kanälen.

Bei Verschluss sind Regelungen zu treffen, die die Zutrittsrechte, die Verteilung der Schlüssel und die Zugriffsmodalitäten festlegen. Weitere Angaben zur geeigneten Aufstellung und Aufbewahrung von IT-Systemen sind unter 11.5 Geeignete Aufstellung und Aufbewahrung zu finden.

11.4.3 Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

Nicht mehr benötigte Leitungen sollten nach Möglichkeit entfernt werden.

Ist dies aufgrund der damit verbundenen Beeinträchtigung des Dienstbetriebes (Öffnen von Decken, Fensterbank- und Fußbodenkanälen) nicht möglich, sind folgende Maßnahmen sinnvoll:

- Kennzeichnen der nicht benötigten Leitungen in der Revisionsdokumentation und Löschen der Eintragungen in der im Verteiler befindlichen Dokumentation,
- Auftrennen aller Rangierungen und Verbindungen der freien Leitungen in den Verteilern (soweit möglich),
- Kurzschließen der freien Leitungen an beiden Kabelenden und in allen berührten Verteilern,
- Auflegen der freien Leitungen auf Erde (Masse) an beiden Kabelenden und in allen berührten Verteilern; bei dadurch entstehenden Masse-Brumm-Schleifen ist nur einseitig zu erden,
- Gewährleisten, dass nicht mehr benötigte Leitungen bei ohnehin anstehenden Arbeiten im Netz entfernt werden.

11.4.4 Auswahl geeigneter Kabeltypen

Bei der Auswahl von Kabeln ist neben der Berücksichtigung von übertragungstechnischen Anforderungen und Umfeldbedingungen auch die Frage nach den Sicherheitsanforderungen zu stellen.

Herkömmliche Kupferleitungen bieten ein potenzielles Ziel für aktive und passive Angriffe. Abhilfe kann hier entweder die Verwendung mehrfach geschirmter Leitungen oder der Einsatz von Lichtwellenleitern bringen.

Lichtwellenleiter sind unempfindlich gegen elektrische und elektromagnetische Störungen und bieten Schutz gegen (aktives und passives) Wiretapping auf der Leitung. Ein potenzielles Angriffsziel stellen aber die Schnittstellen (etwa Verstärker) dar, hier sind bei Bedarf entsprechende Schutzvorkehrungen zu treffen.

Vgl. dazu auch 11.3.8 Schutz gegen kompromittierende Abstrahlung.

11.4.5 Schadensmindernde Kabelführung

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollen Trassen nur in den Bereichen verlegt werden, die ausschließlich den BenutzerInnen zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollen immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Der Standort von Geräten sollte so gewählt werden, dass Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.

In Tiefgaragen ist darauf zu achten, dass durch Trassen im Fahrbereich die zulässige Fahrzeughöhe nicht unterschritten wird, und dass Fremdpersonen keinen unautorisierten Zugriff zu den - in der Regel in geringer Deckenhöhe verlaufenden - Trassen erhalten.

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fußbodenkanälen durch deren Bereiche führen. Fußboden- und Fensterbank-Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.

Bereiche mit hoher Brandgefahr sind zu meiden. Ist dies nicht möglich und ist der Betriebserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung (siehe auch 11.2.4 Brandabschottung von Trassen) zu versehen. Ist der Betriebserhalt nur für einzelne Kabel erforderlich, ist dafür ein entsprechendes Kabel zu wählen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das Gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

11.4.6 Vermeidung von wasserführenden Leitungen

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z. B. Server) befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes/ Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind Wasserleitungen unvermeidbar, kann als Minimalschutz eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden früher entdeckt wird.

Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes/Bereiches einzubauen und müssen stromlos geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich ggf. eine selbsttätige Entwässerung.

11.5 Geeignete Aufstellung und Aufbewahrung

Bei der Aufstellung eines IT-Systems sind verschiedene Voraussetzungen zu beachten, die die Sicherheit des Systems gewährleisten bzw. erhöhen sollen. Über diese Sicherheitsaspekte (die naturgemäß den Schwerpunkt des vorliegenden Handbuches bilden) hinaus, sollen durch eine geeignete Aufstellung auch die Lebensdauer und Zuverlässigkeit der Technik sowie die Ergonomie des Systems verbessert werden.

Im Folgenden werden generelle Hinweise für die Aufstellung von IT-Systemen und Komponenten gegeben, wie sie für die mittlere Datenverarbeitung typisch sind. Dabei wird unterschieden zwischen:

- Arbeitsplatz-IT-Systemen (11.5.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems: PCs, Notebooks, Telearbeitsplätze, …)
- Server (11.5.2 Geeignete Aufstellung eines Servers: neben Datenbankservern, Kommunikationsservern etc. sind davon auch Telekommunikationsanlagen umfasst)
- Netzwerkkomponenten (11.5.3 Geeignete Aufstellung von Netzwerkkomponenten: z. B. Modems, Switches/Router, Verteilerschränke, …)

Wie für das gesamte Handbuch zutreffend und bereits in der Einleitung ausgeführt, wird auch hier nicht auf den Bereich des klassischen Rechenzentrums eingegangen, da hier i. Allg. sehr produkt- und herstellerspezifische Anforderungen bestehen und diese zudem über die Maßnahmen für den mittleren Schutzbedarf hinausgehen und damit den Rahmen der vorliegenden Arbeit sprengen würden.

Es ist festzuhalten, dass eine generelle Klassifikation aller IT-Komponenten in eine der oben genannten Gruppen nicht möglich ist.

Die unten angeführten Maßnahmen sind daher als allgemeine Hinweise zu verstehen, die auf die Bedürfnisse des speziellen Falles abzubilden sind.

11.5.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems

Unter Arbeitsplatz-IT-Systemen sind etwa PCs, Notebooks oder Terminals/„Thin Clients“ zu verstehen.

Bei der Aufstellung eines Arbeitsplatz-IT-Systems sollten - zusätzlich zu den von den Herstellern festgeschriebenen Vorgaben und Hinweisen sowie ergonomischen Gesichtspunkten - unter anderem folgende Voraussetzungen beachtet werden:

- der Standort in der Nähe eines Fensters oder einer Tür erhöht die Gefahr des Beobachtens von außerhalb,
- das System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden (Vermeidung von Überhitzung, aber auch kompromittierender Abstrahlung, vgl. 11.3.8 Schutz gegen kompromittierende Abstrahlung),
- das System sollte soweit möglich und erforderlich, physisch gesichert sein (Diebstahlschutz, versperrbare Laufwerke, …, vgl. auch 7.1.7 Clear-Desk-Policy).

11.5.2 Geeignete Aufstellung eines Servers

Unter Servern sind in diesem Zusammenhang etwa Datenbank-, Programm- und Kommunikationsserver, aber auch TK-Anlagen zu verstehen.

Um Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb von Servern sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen.

Diese kann realisiert werden als:

- Serverraum (vgl. 11.5.6 Serverräume):
  Raum zur Unterbringung von Servern, serverspezifischen Unterlagen, Datenträgern in kleinem Umfang sowie weiterer Hardware (etwa Drucker oder Netzwerkkomponenten). Im Serverraum ist i. Allg. kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten.
- Serverschrank, wenn kein separater Serverraum zur Verfügung steht (vgl. 11.5.7 Beschaffung und Einsatz geeigneter Schutzschränke):
  Serverschränke dienen zur Unterbringung von IT-Geräten und sollen den Inhalt sowohl gegen unbefugten Zugriff als auch gegen die Einwirkung von Feuer oder schädigenden Stoffen (Staub, Gase, …) schützen.

Details zu den technischen und organisatorischen Sicherheitsmaßnahmen bei Serverräumen und Serverschränken finden sich in 11.5.6 Serverräume und 11.5.7 Beschaffung und Einsatz geeigneter Schutzschränke.

Generell ist zu beachten:

- Der Zugang und Zugriff zu Servern darf ausschließlich autorisierten Personen möglich sein.
- Eine Vertretungsregelung muss sicherstellen, dass der Zugriff zum Server auch im Vertretungsfall geregelt möglich ist, und unautorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.

11.5.3 Geeignete Aufstellung von Netzwerkkomponenten

Unter Netzwerkkomponenten sind beispielsweise Modems, Switches/Router und Verteilerschränke zu verstehen.

Um den Missbrauch von Netzwerkkomponenten zu verhindern, muss sichergestellt werden, dass nur Berechtigte physikalischen Zugriff darauf haben. So bedeutet etwa der Missbrauch eines Modems zum einem die Durchführung unbefugter Datenübertragungen, durch die Kapazität beeinträchtigt, Schadsoftware eingeschleppt oder Interna nach außen transferiert werden können, zum anderen das unbefugte Ändern oder Auslesen der Modemkonfiguration, wodurch Sicherheitslücken entstehen können.

Steht ein Modem direkt an einem Arbeitsplatz-IT-System zur Verfügung, so ist der physikalische Zugriff darauf abzusichern (z. B. durch Versperren des Raumes, vgl. auch 11.5.1 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems).

Wenn über ein Modem oder einen Modempool Zugänge zum internen Netz geschaffen werden, ist darauf zu achten, dass keine Umgehung einer bestehenden Firewall geschaffen wird. Sollen mit einem Modempool weitere externe Zugänge zu einem durch eine Firewall geschützten Netz geschaffen werden, muss dieser auf der unsicheren Seite der Firewall aufgestellt werden.

Netzwerkkomponenten sollten wie Server in einem gesicherten Serverraum oder einem Schutzschrank aufgestellt sein. Die entsprechenden Maßnahmen 11.5.6 Serverräume und 11.5.7 Beschaffung und Einsatz geeigneter Schutzschränke sind zu beachten.

Auch hier ist sicherzustellen:

- Der Zugang und Zugriff zu Netzwerkkomponenten darf ausschließlich autorisierten Personen möglich sein.
- Eine Vertretungsregelung muss sicherstellen, dass der Zugriff zu Netzwerkkomponenten auch im Vertretungsfall geregelt möglich ist und unautorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.

11.5.4 Nutzung und Aufbewahrung mobiler IT-Geräte

Unter mobilen IT-Geräten sind alle für einen mobilen Einsatz geeigneten Geräte zu verstehen, so etwa Notebooks, Tablets und Smartphones.

Da die Umfeldbedingungen bei mobilem Einsatz meist außerhalb der direkten Einflussnahme der BenutzerInnen liegen, müssen sie versuchen, mobile IT-Geräte auch außer Haus sicher aufzubewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Die BenutzerInnen mobiler IT-Geräte sind über die potenziellen Gefahren bei Mitnahme und Nutzung eines solchen Gerätes außerhalb der geschützten Umgebung eingehend zu informieren und zu sensibilisieren. Soweit möglich sollten solche Informationen in schriftlicher Form - etwa als Merkblätter - an die MitarbeiterInnen verteilt werden. Dabei ist auch auf die besonderen Gegebenheiten in verschiedenen Zielgebieten und in speziellen Situationen (etwa bei einer besonders eingehenden Zollkontrolle) hinzuweisen.
- Werden auf mobilen IT-Geräten eingeschränkte, vertrauliche, geheime oder streng geheime bzw. personenbezogene oder sensible Daten (siehe 8.2.1 Definition der Sicherheitsklassen) gespeichert und verarbeitet, so ist die Installation eines Zugriffsschutzes (über Passwort oder Chipkarte) sowie einer Festplatten- oder Dateiverschlüsselung dringend zu empfehlen (vgl. auch 8.1.3.1 Herausgabe einer PC-Richtlinie). Dabei ist zu beachten, dass die Zulässigkeit von Verschlüsselungstechnologien in den einzelnen Staaten unterschiedlich geregelt ist.
- Soweit möglich, sollten auch mobile Datenträger (z. B. USB-Sticks) ausschließlich chiffrierte Daten enthalten; werden in Ausnahmefällen unverschlüsselte Datenträger im mobilen Einsatz verwendet, so sollten diese keinesfalls unbeaufsichtigt (etwa im Hotel oder in einem Fahrzeug) zurückgelassen werden.
- Nach Möglichkeit sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden.
- Werden mobile IT-Geräte in einem Kraftfahrzeug aufbewahrt, so sollten diese Geräte von außen nicht sichtbar sein. Das Abdecken der Geräte oder das Einschließen in den Kofferraum bieten Abhilfe.
- Wird ein mobiles IT-Gerät in fremden Büroräumen vor Ort benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das Gerät ausgeschaltet werden, um über das Bootpasswort die unerlaubte Nutzung zu verhindern.
- In Hotelräumen sollte ein mobiles IT-Gerät nicht offen aufliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.
- Einige Geräte bieten zusätzlich die Möglichkeit zum Anketten des Gerätes. Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.

- Falls für die jeweiligen mobilen Geräte eine Möglichkeit zur Ortung (z.B. über GPS-, IP- oder WLAN-Ortung) existiert, kann diese zum Auffinden nach erfolgtem Diebstahl oder Verlust zu Hilfe genommen werden. Hierbei sind jedoch zwingend Vertraulichkeits- und datenschutzrechtliche Aspekte zu beachten.

11.5.5 Sichere Aufbewahrung der Datenträger vor und nach Versand

Vor dem Versand eines Datenträgers ist zu gewährleisten, dass für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Beschriebene Datenträger sollten bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z. B. Poststelle) sind auf die sachgerechte und sichere Aufbewahrung und Handhabung von Datenträgern hinzuweisen.

Alternativ oder ergänzend kann auch eine verschlüsselte Speicherung der Daten vorgenommen werden.

Weitere Maßnahmen dazu finden sich in 8.3 Betriebsmittel und Datenträger.

11.5.6 Serverräume

Ein Serverraum dient zur Unterbringung eines oder mehrerer Server sowie serverspezifischer Unterlagen. Darüber hinaus können dort auch Datenträger (in kleinerem Umfang) sowie zusätzliche Hardware, wie etwa Protokolldrucker oder Klimatechnik, vorhanden sein.

Im Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als beispielsweise in einem Büroraum.

Für den Schutz von Serverräumen sind die entsprechenden baulichen und infrastrukturellen Maßnahmen, die in 11.1 Bauliche und infrastrukturelle Maßnahmen beschrieben werden, zur Anwendung zu bringen. Besondere Beachtung ist dabei folgenden Maßnahmen zu widmen:

- 11.1.4 Zutrittskontrolle
- 11.2.2 Raumbelegung unter Berücksichtigung von Brandlasten
- 11.2.8 Handfeuerlöscher
- 11.2.11 Rauchverbot
- 11.3.2 Not-Aus-Schalter
- 11.3.4 Lokale unterbrechungsfreie Stromversorgung

- 11.3.6 Überspannungsschutz (Innerer Blitzschutz)
- 11.4.6 Vermeidung von wasserführenden Leitung
- 11.6.4 Geschlossene Fenster und Türen
- 11.6.5 Alarmanlage
- 11.6.6 Fernanzeige von Störungen
- 11.6.7 Klimatisierung
- 7.2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

11.5.7 Beschaffung und Einsatz geeigneter Schutzschränke

Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen.

Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

- Schutz gegen Feuereinwirkung:
  Bei Schutzschränken unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120 nach ÖNORM EN 1047-1. In diesen Güteklassen werden die Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120 Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im Einzelnen:
  P = Papier aller Art,
  D = Datenträger (z. B. Magnetbänder, Filme),
  DIS = Disketten und Magnetbandkassetten einschließlich aller anderen Datenträger.
  Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei DIS-Schränken am höchsten ist. Für den IT-Grundschutz sollten bei Schutz gegen Feuer Schutzschränke der Güteklasse S60 ausreichend sein. Zu beachten bleibt, dass solche Schränke damit Schutz gegen Feuer für einen gewissen Zeitraum bieten, so dass Datenträger nicht zerstört werden, jedoch ist davon auszugehen, dass im Brandfall der Betrieb eines in einem Serverschrank untergebrachten Servers nicht aufrechterhalten werden kann. Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine Vorrichtung zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die Schließung sollte lokal durch Rauchgasmelder oder extern durch ein Signal einer Brandmeldeanlage (soweit vorhanden) ausgelöst werden können.
- Schutz gegen unbefugten Zugriff:

Der Schutzwert gegen unbefugten Zugriff wird neben der mechanischen Festigkeit des Schutzschrankes entscheidend durch die Güte des Schlosses beeinflusst. Für den IT-Grundschutz sind Wertschränke geeignet, die durch ECB-S (C 01) oder VdS (2450), auf Basis der europäischen Norm EN 1143-1, zertifiziert wurden. Die Wahl des Widerstandsgrades hängt vom konkreten Einsatzbereich und Schutzbedarf ab.

Die ehemals für Stahlschränke weit verbreitete Norm VDMA 24992 des Verbandes deutscher Maschinen- und Anlagenbau e.V. (VDMA) wurde vor geraumer Zeit ersatzlos zurückgezogen.

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung am Aufstellungsort zu berücksichtigen. Schutzschränke, die aufgrund ihrer geringen Größe relativ einfach weggetragen werden könnten, sollten in der Wand oder im Boden verankert werden.

Nach diesen Auswahlkriterien für den Schutzwert des Schutzschrankes ist als Nächstes die Ausstattung des Schrankes bedarfsgerecht festzulegen. Dazu sollte vor der Beschaffung eines Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

Serverschränke:
Schutzschränke, in denen wichtige IT-Komponenten (also im Regelfall Server) untergebracht sind, werden auch als Serverschränke bezeichnet. In diesen sollte außer für den Server und eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z. B. externe Festplatten oder Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, dass die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebracht wird, dass AdministratorInnen Arbeiten sitzend durchführen können. Je nach Nutzung des Schrankes können auch eine Klimatisierung oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muss zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- **und** der Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

Nicht im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle der AdministratorInnen. Es ist also nicht sinnvoll, ihnen, ggf. sogar als Einzigen, Zugriff auf die Protokollausdrucke zu gewähren.

Verschluss von Schutzschränken:
Generell sind Schutzschränke bei Nichtbenutzung zu verschließen. Werden Arbeiten, die ein Öffnen des Schutzschrankes erfordern, unterbrochen, so ist auch bei kurzfristigem Verlassen des Raumes der Schutzschrank zu verschließen.

Werden Schutzschränke mit mechanischen oder elektronischen Codeschlössern verwendet, so muss der Code für diese Schlösser geändert werden

- nach der Beschaffung,
- bei Wechsel der BenutzerInnen,
- nach Öffnung in Abwesenheit der BenutzerInnen,
- wenn der Verdacht besteht, dass der Code Unbefugten bekannt wurde und
- mindestens einmal alle zwölf Monate.

Der Code darf nicht aus leicht zu ermittelnden Zahlen (z. B. persönliche Daten, arithmetische Reihen) bestehen.

Die jeweils gültigen Codes von Codeschlössern sind aufzuzeichnen und gesichert zu hinterlegen. Zu beachten ist, dass eine Hinterlegung im zugehörigen Schutzschrank sinnlos ist.

Wenn der Schutzschrank neben einem Codeschloss ein weiteres Schloss besitzt, so ist abzuwägen, ob Code und Schlüssel gemeinsam hinterlegt werden, was im Notfall einen schnelleren Zugriff erlauben würde, oder getrennt hinterlegt werden, so dass es für AngreiferInnen schwieriger ist, sich Zugriff zu verschaffen.

11.6 Weitere Schutzmaßnahmen

11.6.1 Einhaltung einschlägiger Normen und Vorschriften

Für nahezu alle Bereiche der Technik gibt es Normen bzw. Vorschriften, z. B. der ÖNORM und des ÖVE. Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für die BenutzerInnen und Sicherheit für den Betrieb gewährleisten. Bei der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

In A.1 Sicherheitsszenarien werden einige dieser Normen beispielhaft angeführt.

11.6.2 Regelungen für Zutritt zu Verteilern

Die Verteiler (z. B. für Energieversorgung, Datennetze, Telefon) sind nach Möglichkeit in Räumen für technische Infrastruktur unterzubringen. Die dort geforderten Maßnahmen sind zu berücksichtigen.

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude muss möglich und geordnet sein.

Mit „möglich“ ist gemeint, dass

- Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, dass sie nur noch mit Werkzeug zu öffnen oder unauffindbar sind,
- Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,
- für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionieren.

Mit „geordnet“ ist gemeint, dass festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schlüssel und entsprechende Schlüsselverwaltung geregelt werden (siehe dazu 11.1.4 Zutrittskontrolle).

11.6.3 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Schützenswerte Gebäudeteile sind z. B. Rechenzentrum, Serverraum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalträume, Ersatzteillager. Solche Bereiche sollten nach Möglichkeit keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z. B. „Rechenzentrum“ oder „EDV-Archiv“ geben einem potenziellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten zu können.

Ist es unvermeidbar, IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch 11.1.2 Anordnung schützenswerter Gebäudeteile), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z. B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

11.6.4 Geschlossene Fenster und Türen

Fenster und nach außen gehende Türen (Balkone, Terrassen) sind in Zeiten, in denen ein Raum nicht besetzt ist, zu schließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen bieten sie EinbrecherInnen auch während der Betriebszeiten eine ideale Einstiegsmöglichkeit. Während normaler Arbeitszeiten und sichergestellter kurzer Abwesenheit der MitarbeiterInnen kann von einer zwingenden Regelung für Büroräume abgesehen werden. Auch nach innen gehende Türen nicht besetzter Räume sollten i. Allg. abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen.

In manchen Fällen, z. B. in Großraumbüros, ist der Verschluss des Büros nicht möglich. In diesem Fall sollte alternativ sämtliche MitarbeiterInnen vor ihrer Abwesenheit Unterlagen und den persönlichen Arbeitsbereich (Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss, Telefon) verschließen (siehe auch 7.1.7 Clear-Desk-Policy).

Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn eine Sicherungsmaßnahme installiert ist, mit der die Nutzung des Rechners nur unter Eingabe eines Passwortes weitergeführt werden kann (passwortunterstützte Bildschirmschoner), der Bildschirminhalt gelöscht wird und das Booten des Rechners die Eingabe eines Passwortes verlangt.

Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn die Inbetriebnahme des Gerätes die Eingabe eines Passwortes verlangt und sichergestellt ist, dass keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen aufliegen.

Es muss auf jeden Fall sichergestellt werden, dass die Passworteingabe keinesfalls umgangen werden kann.

11.6.5 Alarmanlage

Ist eine Alarmanlage für Einbruch oder Brand vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, ist zu überlegen, ob zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden sollen. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung der Alarmanlage vorzusehen.

Ist keine Alarmanlage vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Melder in Betracht. Diese arbeiten völlig selbstständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (evtl. Telefonleitung) an anderer Stelle.

Weiters ist zu beachten:

- Die Alarmanlage muss regelmäßig gewartet bzw. geprüft werden.
- Die zuständigen Personen sind über die im Alarmfall einzuleitenden Schritte zu unterrichten.
- Besonders wirksam ist „Stiller Alarm mit Rückfrage“, dies erfordert jedoch zusätzlichen organisatorischen Aufwand.

11.6.6 Fernanzeige von Störungen

IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfordern, werden oft in ge- und verschlossenen Räumen untergebracht (z. B. Serverraum). Das führt dazu, dass Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirken und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entdeckt werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche „schleichenden“ Gefährdungen angeführt.

Durch eine Fernanzeige ist es möglich, solche Störungen früher zu erkennen. Viele Geräte, auf die man sich verlassen muss, ohne sie ständig prüfen oder beobachten zu können, haben heute einen Anschluss für Störungsfernanzeigen. Die technischen Möglichkeiten reichen dabei von einfachen Kontakten, über die eine Warnlampe eingeschaltet werden kann, bis zu Rechnerschnittstellen mit dazugehörigem Softwarepaket für die gängigen Betriebssysteme. Über die Schnittstellen ist es oft sogar möglich, jederzeit den aktuellen Betriebszustand der angeschlossenen Geräte festzustellen und so Ausfällen rechtzeitig begegnen zu können.

11.6.7 Klimatisierung

Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur durch Kühlung unter dem von der IT vorgegebenen Höchstwert zu halten.

Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen. Dazu muss das Klimagerät allerdings an eine Wasserleitung angeschlossen werden. 11.4.6 Vermeidung von wasserführenden Leitungen ist zu beachten.

Zusätzlich ist zu beachten, dass die Luftumwälzung durch eine Klimaanlage auch Emissionen aus der Umgebung in die Nähe von empfindlichen IT-Komponenten bringen kann. So ist etwa bei baulichen Maßnahmen, insbesondere bei Umbauarbeiten in bestehenden Räumen und Gebäuden, darauf zu achten, dass Kleber, Anstriche etc. säurefrei sind, um eine Korrosion von IT-Bauteilen durch vorbeigeführte Luft aus der Klimaanlage zu vermeiden.

Um die Schutzwirkung aufrechtzuerhalten ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen.

11.6.8 Selbsttätige Entwässerung

Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und ggf. mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a. Keller, Lufträume unter Doppelböden, Lichtschächte und Heizungsanlagen.

11.6.9 Videounterstützte Überwachung

Zur besseren Absicherung der Infrastruktur sollte bei Bedarf auf ein videounterstütztes Überwachungssystem zurückgegriffen werden.

Derartige Überwachungssysteme stellen eine sinnvolle Ergänzung der bestehenden Maßnahmen (vgl. 11.6 Weitere Schutzmaßnahmen) dar. Bei geeigneter Aufstellung ist auch die von Überwachungskameras ausgehende Abschreckung ein Vorteil derartiger Systeme. Im Zuge der Konzeption und Installation müssen Personal sowie zusätzliche technische und infrastrukturelle Vorkehrungen zur Auswertung vorgesehen werden.

Die Wahl der Aufstellungsplätze der Kameras sollte unter Beiziehung des Betriebsrates und unter Berücksichtigung des Datenschutzes erfolgen.

11.6.10 Aktualität von Plänen

Sämtliche Pläne sind aktuell zu halten und an geeigneten Stellen zu deponieren.

Nach jedem Eingriff der eine Aktualisierung der Pläne erforderlich macht (bauliche Maßnahmen o.ä.), sind diese umgehend auf den aktuellen Stand zu bringen.
In diesem Zuge sind auch alle in Umlauf befindlichen Kopien der Pläne durch aktualisierte Kopien zu ersetzen.

11.6.11 Vorgaben für ein Rechenzentrum

> *Ein Rechenzentrum gilt als schützenswert und sollte daher im Sinne eines Sicherheitsbereiches konzipiert sein.*

In diesem Zusammenhang sind die in 11.1 Bauliche und infrastrukturelle Maßnahmen getroffenen Maßnahmen von besonderer Bedeutung. Aus diesem Katalog sollten folgende Punkte besonders beachtet werden:

- geeignete Standortwahl (11.1.1 Geeignete Standortauswahl)
- ausreichender Einbruchsschutz (11.1.3 Einbruchsschutz)
- Zutrittskontrollen (11.1.4 Zutrittskontrolle)
- Aufstellung und Anordnung von Geräten (11.5 Geeignete Aufstellung und Aufbewahrung)

Weiters ist zu beachten:

- Verfügbarkeitsanforderungen (17.1.1 Definition von Verfügbarkeitsklassen)

12 Sicherheitsmanagement im Betrieb

12.1 IT-Sicherheitsmanagement

Informationssicherheitsmanagement steht für eine kontinuierliche Planungs- und Lenkungsaufgabe zur Umsetzung eines wirksamen Prozesses mit dem Ziel, ein umfassendes, angemessenes und konsistentes Informationssicherheitsniveau für die gesamte Organisation herzustellen und zu erhalten. Die Umsetzung der in diesem Kapitel angeführten Maßnahmen soll dies gewährleisten.

12.1.1 Etablierung eines IT-Sicherheitsmanagementprozesses

Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener IT-Sicherheit unerlässlich. Der IT-Sicherheitsmanagementprozess ist daher ein integraler Bestandteil der organisationsweiten IT-Sicherheitspolitik (vgl. 12.1.2 Erarbeitung einer organisationsweiten IT-Sicherheitspolitik, und in dem Zusammenhang auch [IKTB-170902-8]). Dabei handelt es sich um einen kontinuierlichen Prozess, der die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Zuverlässigkeit von IT-Systemen gewährleisten soll. Dieser Prozess ist zumindest auf Ebene der Gesamtorganisation zu etablieren, über eine Durchführung auf der Ebene einzelner Organisationseinheiten ist im Einzelfall zu entscheiden.

Zu den Aufgaben des IT-Sicherheitsmanagements gehören:

- Festlegung der IT-Sicherheitsziele, -strategien und -politiken der Organisation,
- Festlegung der IT-Sicherheitsanforderungen,
- Ermittlung und Analyse von Bedrohungen und Risiken,
- Festlegung geeigneter Sicherheitsmaßnahmen,
- Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Maßnahmen,
- Förderung des Sicherheitsbewusstseins innerhalb der Organisation sowie
- Entdecken von und Reaktion auf sicherheitsrelevante Ereignisse.

Die folgende Graphik zeigt die wichtigsten Aktivitäten im Rahmen des Informationssicherheitsmanagements und die eventuell erforderlichen Rückkopplungen zwischen den einzelnen Stufen. In 2.1 Informationssicherheitsmanagement-Prozess werden die zur Etablierung eines umfassenden Informationssicherheitsmanagementprozesses erforderlichen Schritte detailliert beschrieben.

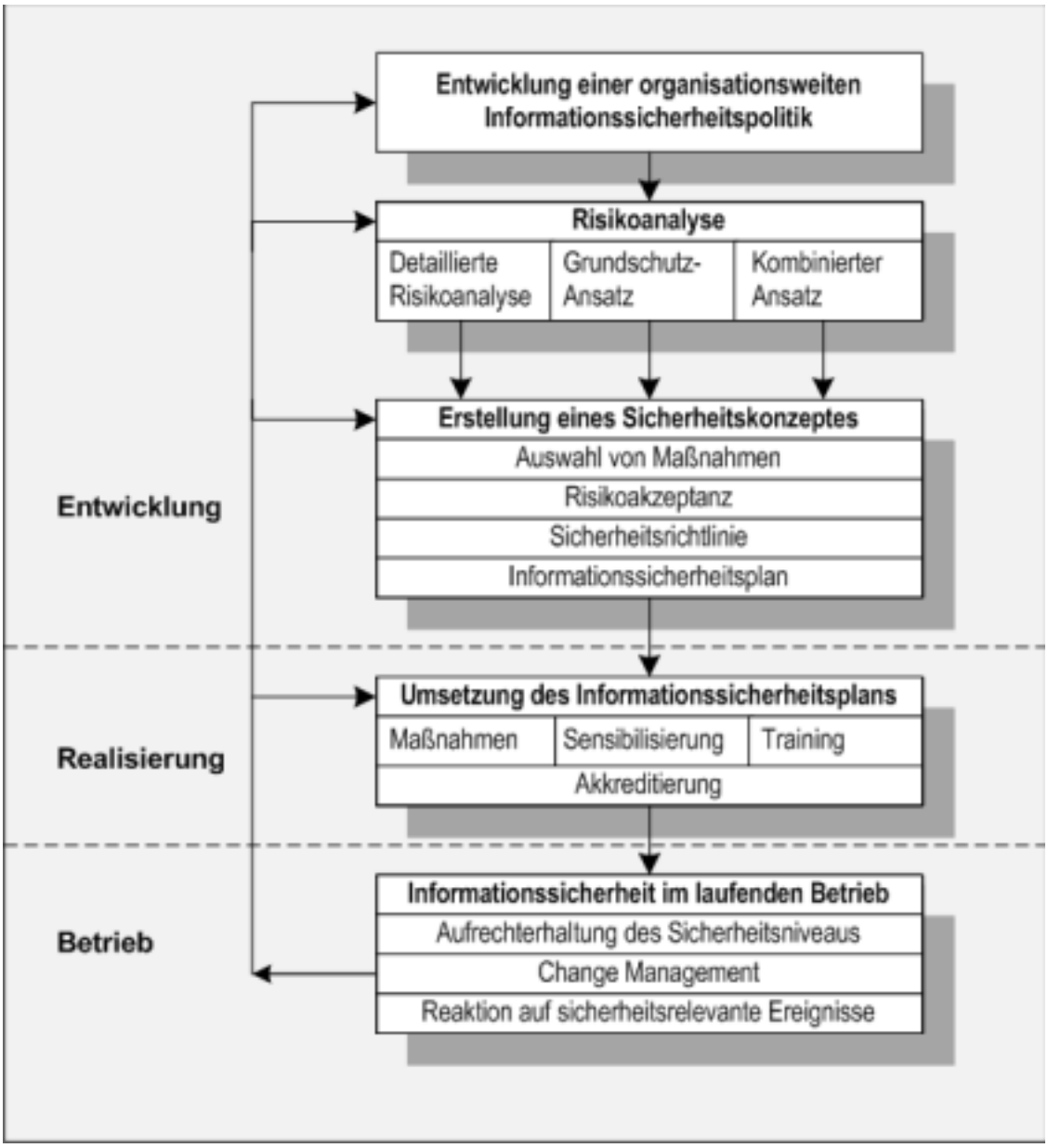

Abbildung 12.1: Aktivitäten im Rahmen des IT-Sicherheitsmanagements

12.1.2 Erarbeitung einer organisationsweiten Informationssicherheitspolitik

Als organisationsweite IT-Sicherheitspolitik bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksichtigung gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der IT-Sicherheit festlegen.

Ressorts in der öffentlichen Verwaltung werden auf Basis des IKT-Board-Beschlusses [IKTB-170902-8] explizit zur Umsetzung einer Sicherheitspolitik angehalten.

Jede Organisation sollte eine in schriftlicher Form vorliegende IT-Sicherheitspolitik erarbeiten, die als langfristig gültiges Dokument zu betrachten ist.

Die organisationsweite Informationssicherheitspolitik soll allgemeine Festlegungen treffen, die für alle Einsatzbereiche der Informationstechnologie innerhalb einer Organisation zur Anwendung kommen und folgende Inhalte umfassen:

- Grundsätzliche Ziele und Strategien
- Organisation und Verantwortlichkeiten für IT-Sicherheit
- Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz
- Klassifikation von Daten
- Organisationsweite Richtlinien zu Sicherheitsmaßnahmen
- Disaster Recovery-Planung
- Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit

Details und Anleitungen zur Erstellung einer organisationsweiten IT-Sicherheitspolitik finden sich in 4 Informationssicherheitspolitik.

In diesem Zusammenhang sei auch auf die Österreichische Strategie für Cyber Sicherheit (ÖSCS) [OESCS] hingewiesen.

12.1.3 Erarbeitung von IT-Systemsicherheitspolitiken

Für jedes IT-System sollte eine IT-Systemsicherheitspolitik erarbeitet werden, welche

- die grundlegenden Vorgaben und Leitlinien zur Sicherheit in diesem System definiert,
- Details über die ausgewählten Sicherheitsmaßnahmen beschreibt und
- die Gründe für die Auswahl der Sicherheitsmaßnahmen dargelegt.

Die IT-Systemsicherheitspolitik sollte Aussagen zu folgenden Bereichen treffen:

- Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Komponenten
- Definition der wichtigsten Ziele und Funktionalitäten des Systems
- Festlegung der IT-Sicherheitsziele des Systems
- Abhängigkeit der Organisation vom betrachteten IT-System
- Investitionen in das System
- Risikoanalysestrategie
- Werte, Bedrohungen und Schwachstellen lt. Risikoanalyse
- Sicherheitsrisiken
- Beschreibung der bestehenden und der noch zu realisierenden Sicherheitsmaßnahmen

- Gründe für die Auswahl der Maßnahmen
- Kostenschätzungen für die Realisierung und Wartung (Aufrechterhaltung) der Sicherheitsmaßnahmen
- Verantwortlichkeiten

Details und Anleitungen zur Erstellung von IT-Systemsicherheitspolitiken finden sich in 4 Informationssicherheitspolitik.

12.1.4 Festlegung von Verantwortlichkeiten

> *Um eine Berücksichtigung aller wichtigen Sicherheitsaspekte und eine effiziente Erledigung sämtlicher anfallender Aufgaben zu gewährleisten, ist es erforderlich, die Rollen aller in den IT-Sicherheitsprozess involvierten Personen klar zu definieren.*

Diese Festlegung erfolgt zweckmäßig im Rahmen der organisationsweiten IT-Sicherheitspolitik (vgl. 12.1.2 Erarbeitung einer organisationsweiten Informationssicherheitspolitik und 4 Informationssicherheitspolitik).

Es empfiehlt sich, darüber hinaus detaillierte Regelungen zu folgenden Bereichen zu treffen:

- Datensicherung,
- Datenarchivierung,
- Datenübertragung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Zutritts-, Zugangs- und Zugriffsberechtigungen,
- Datenträger- und Betriebsmittelverwaltung,
- Anwendungsentwicklung,
- Kauf und Leasing von Hardware und Software,
- Abnahme und Freigabe von Software,
- Wartungs- und Reparaturarbeiten,
- Datenschutz,
- Schutz gegen Software mit Schadensfunktion (Viren, Würmer, trojanische Pferde, …)
- Revision,
- Notfallvorsorge und
- Vorgehensweise bei Verletzung der Sicherheitspolitik.

Nähere Erläuterungen dazu finden sich in den nachfolgenden Maßnahmenbeschreibungen.

Weiters ist zu beachten:

- Die Regelungen sind den betroffenen MitarbeiterInnen in geeigneter Weise bekannt zu geben.
- Sämtliche Regelungen sind in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.
- Es empfiehlt sich, die Bekanntgabe zu dokumentieren.
- Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu verhindern.

12.1.5 Funktionstrennung

Im Rahmen der Zuordnung von Aufgaben und Verantwortlichkeiten ist auch festzulegen, welche Funktionen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen („Funktionstrennung“).

Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. Beispiele dafür sind:

- Rechteverwaltung und Revision,
- Netzadministration und Revision,
- Programmierung und Test bei eigenerstellter Software,
- Datenerfassung und Zahlungsanordnungsbefugnis,
- Revision und Zahlungsanordnungsbefugnis.

Insbesondere wird deutlich, dass meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.

Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Die dabei getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen im IT-Einsatz zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

12.1.6 Einrichtung von Standardarbeitsplätzen

Ein Standardarbeitsplatz ist gekennzeichnet durch einheitliche Hardware und Software sowie deren Konfiguration. Die Planung und Einrichtung erfolgt üblicherweise unter den Aspekten der Aufgabenstellung, Zuverlässigkeit, Ergonomie, Geschwindigkeit und Wartbarkeit. Sie wird durch fachkundiges Personal durchgeführt.

In Anlehnung an den IKT-Board-Beschluss vom 17.09.2002 [IKTB-170902-7] wird die Verwendung und Umsetzung einer sicheren Initialkonfiguration bei der Auslieferung von Systemen im Bundesbereich empfohlen. Dadurch soll das Vertrauen in das Grundsystem gestärkt werden.

Die Einrichtung von Standardarbeitsplätzen ist in mehrfacher Hinsicht vorteilhaft:

IT-Sicherheit:

- Standardarbeitsplätze sind leichter in Sicherheitskonzepte einzubinden.
- Der Aufwand für die Dokumentation des IT-Bestandes wird reduziert.

IT-Management:

- Die Beschaffung größerer Stückzahlen gleicher Komponenten ermöglicht Preisvorteile.
- Der Einsatz nicht zulässiger Software ist einfacher festzustellen.
- Durch gleiche IT-Ausstattung entfallen „Neidfaktoren“ zwischen den einzelnen BenutzerInnen.

IT-NutzerInnen:

- Bei Gerätewechsel ist keine erneute Einweisung in die IT-Konfiguration erforderlich, Ausfallzeiten werden somit minimiert.
- Bei Fragen zu Hard- und Software können sich AnwenderInnen gegenseitig helfen.

Systemadministration bei Installation und Wartung:

- Eine gewissenhaft geplante und getestete Installation kann fehlerfrei und mit geringem Arbeitsaufwand installiert werden.
- Die einheitliche Arbeitsumgebung erleichtert Wartung und Support.

Schulung:

- Die TeilnehmerInnen werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

12.1.7 Akkreditierung von IT-Systemen

Für jedes IT-System ist sicherzustellen, dass es den Anforderungen der IT-Systemsicherheitspolitik genügt.

Dabei ist insbesondere darauf zu achten, dass die Sicherheit des Systems

- in einer bestimmten Betriebsumgebung,
- unter bestimmten Einsatzbedingungen und
- für eine bestimmte vorgegebene Zeitspanne

gewährleistet ist.

Erst nach erfolgter Akkreditierung kann das System - oder gegebenenfalls eine spezifische Anwendung - in Echtbetrieb gehen.

Techniken zur Akkreditierung sind:

- Prüfung der Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspolitik (Security Compliance Checking), vgl. auch 18.1 Security Compliance Checking und Monitoring
- Tests
- Evaluation und Zertifizierung von Systemen

Änderungen der eingesetzten Sicherheitsmaßnahmen oder der Betriebsumgebung können eine neuerliche Akkreditierung des Systems erforderlich machen. Die Kriterien, wann eine Neuakkreditierung durchzuführen ist, sollten in der IT-Systemsicherheitspolitik festgelegt werden.

12.1.8 Change Management

Aufgabe des Change Managements ist es, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen am IT-System ergeben. Sind signifikante Hardware- oder Softwareänderungen in einem IT-System geplant, so sind die Auswirkungen auf die Gesamtsicherheit des Systems zu untersuchen.

Im Rahmen des Konfigurationsmanagements ist sicherzustellen, dass Änderungen an einem IT-System nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen und damit einer Gefährdung der Gesamtsicherheit führen.

12.1.8.1 Reaktion auf Änderungen am IT-System

Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird.

Dazu gehören zum Beispiel:

- Änderungen des IT-Systems (neue Applikationen, neue Hardware, neue Netzwerkverbindungen, …),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- räumliche Änderungen, z. B. nach einem Umzug,

- Änderungen in der Bewertung der eingesetzten IT, der notwendigen Vertraulichkeit, Integrität oder Verfügbarkeit und
- Änderungen bei Bedrohungen oder Schwachstellen.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind schriftlich zu dokumentieren.

Abhängig von der Bedeutung des Systems und dem Grad der Änderung kann eine neuerliche Durchführung vorangegangener Aktivitäten im Sicherheitsprozess (vgl. 12.1.1 Etablierung eines IT-Sicherheitsmanagementprozesses erforderlich werden.

Eine Änderung des IT-Systems oder seiner Einsatzbedingungen kann also

- Änderungen in der Umsetzung des Informationssicherheitsplans,
- die Erstellung eines neuen Sicherheitskonzeptes,
- eine neue Risikoanalyse oder sogar
- die Überarbeitung der organisationsweiten Informationssicherheitspolitik

erforderlich machen.

12.1.8.2 Softwareänderungskontrolle

> *Softwareänderungskontrolle (Software Change Control) ist der Teil des Change Managements, der sich auf die Gewährleistung der Integrität von Software bei Änderungen bezieht.*

Es ist sicherzustellen, dass

- nur abgenommene und freigegebene Software installiert wird (vgl. 14.1.7 Abnahme und Freigabe von Software),
- die freigegebene Software(version) nur unverändert installiert werden kann (vgl. 14.1.9 Sicherstellen der Integrität von Software),
- Installation und Konfiguration entsprechend den Installationsanweisungen erfolgen (vgl. 14.1.8 Installation und Konfiguration von Software) und
- Standardsoftware einer Lizenzverwaltung und Versionskontrolle unterliegt (vgl. 14.1.10 Lizenzverwaltung und Versionskontrolle von Standardsoftware).

Für komplexe Eigenentwicklungen empfiehlt sich die Erstellung eines „Softwarepflege- und -änderungskonzeptes“ (SWPÄ-Konzept, vgl. 14.3.6 Softwarepflege- und -änderungskonzept).

12.2 Dokumentation

Die im Folgenden angeführten Maßnahmen geben grobe Richtlinien zu den Anforderungen an die Dokumentation. Dabei wird insbesondere auf die sicherheitsspezifischen Fragen im Rahmen der Dokumentation eingegangen. Die Ausführungen orientieren sich an den „Allgemeinen Vertragsbedingungen der Republik Österreich für IT-Leistungen“ [AVB-IT], dem „Vorgehensmodell für die Entwicklung von IT-Systemen des Bundes“ [IT-BVM] sowie den [Common Criteria]. In den genannten Dokumenten finden sich auch weitere Details.

12.2.1 Dokumentation von Software

Für jede Softwarekomponente ist die Verfügbarkeit der zu ihrer Nutzung erforderlichen und zweckmäßigen Dokumentation sicherzustellen.

Dabei ist zu achten auf:

- die Vollständigkeit und Korrektheit der gelieferten Dokumentation und
- die laufende Aktualisierung der Dokumentation während der gesamten Nutzungsdauer der Software.

Die Dokumentation muss zumindest beinhalten:

- Benutzerdokumentation
- Dokumentation für Installation und Administration

Darüber hinaus können je nach Bedarf folgende Anforderungen bestehen:

- technische Dokumentation
- Entwicklungsdokumentation

Benutzerdokumentation:

Bei der Benutzerdokumentation (in den [IT-BVM] als „Anwendungshandbuch“ bezeichnet) handelt es sich um Information über die Software, die die EntwicklerInnen den BenutzerInnen zur Verwendung bereitstellen.

Die Benutzerdokumentation hat alle für die laufende Arbeit notwendigen Abläufe so zu beschreiben, dass sie für eine eingeschulte Person verständlich sind. Daneben hat die Dokumentation typische und vorhersehbare Fehlersituationen und deren Behebung zu beschreiben.

Aus sicherheitstechnischer Sicht soll die Benutzerdokumentation den EndbenutzerInnen helfen,

- die Sicherheitseigenschaften der Software sowie
- den Beitrag der EndbenutzerInnen zur Gewährleistung der Sicherheit bei der Verwendung der Software

zu verstehen.

Die Benutzerdokumentation sollte in deutscher Sprache vorliegen. Dies kann und sollte auch vertraglich festgelegt werden (vgl. etwa [AVB-IT]).

Ebenso empfiehlt sich eine Vereinbarung über die Lieferung der Dokumentation zusätzlich in maschinenlesbarer Form, so dass diese an definierten Arbeitsplätzen während der Arbeit abgerufen werden kann.

Dokumentation für Installation und Administration:

Bei dieser Dokumentation handelt es sich um Information über die erforderlichen Maßnahmen zur Aufnahme des Betriebs, zur Durchführung und Überwachung des Betriebs und zur Unterbrechung und Beendigung des Betriebs. Sie soll AdministratorInnen helfen, die Software in einer sicheren Art und Weise zu installieren, zu konfigurieren und zu bedienen.

Die Dokumentation für die Installation und Administration (im Folgenden kurz als „Administratordokumentation“, in den [IT-BVM] als „Betriebshandbuch“ bezeichnet) hat alle für die Installation und die laufende Verwaltung des Systems notwendigen Abläufe so zu beschreiben, dass sie für eine eingeschulte Person verständlich sind. Daneben hat die Dokumentation typische und vorhersehbare Fehlersituationen und deren Behebung zu beschreiben.

Aus sicherheitstechnischer Sicht muss die Administratordokumentation die sicherheitsspezifischen Funktionen darlegen, die für AdministratorInnen von Bedeutung sind. Darüber hinaus muss sie Richtlinien zur konsistenten und wirksamen Nutzung der Sicherheitseigenschaften der Software enthalten und darlegen, wie solche Eigenschaften zusammenwirken.

Technische Dokumentation:

Diese muss den zum Zeitpunkt der Installation der Software üblichen Standards entsprechen und so gestaltet sein, dass sie für mit ähnlichen Komponenten vertraute ExpertInnen verständlich und verwertbar ist.

12.2.2 Sourcecodehinterlegung

Im Falle einer Lieferung von Software, bei der der Sourcecode nicht mitgeliefert wird, sollte nach Möglichkeit - insbesondere bei der Entwicklung von Individualsoftware - Sourcecodehinterlegung vereinbart werden.

Diese soll die Möglichkeit einer weiteren Fehlerbehebung, Änderung und Wartung von Software für den Fall der Handlungsunfähigkeit des Softwareherstellers und den Fall der Einstellung der Weiterentwicklung oder Wartung sicherstellen.

Durchführung:

Die AuftragnehmerInnen (SW-Hersteller) stellen die Software auf einem Datenträger, der auf dem System der/des Auftraggeberin/Auftraggebers gelesen werden kann, in der Quellensprache bereit, übersetzen sie in Maschinencode und nehmen die Installation auf dem System vor.

Nach der Installation wird der Datenträger mit dem Quellencode samt der dazugehörigen Dokumentation (Inhalt und Aufbau des Datenträgers, Programm und Datenflusspläne, Testverfahren, Testprogramme, Fehlerbehandlung usw.) von den AuftragnehmerInnen versiegelt und bei den AuftraggeberInnen oder vertrauenswürdigen Dritten (z. B. NotarInnen) hinterlegt.

Tritt beim Hersteller Handlungsunfähigkeit (etwa Liquidation, Eröffnung eines Konkursverfahrens, …) ein oder stellt sie/er entgegen anders lautenden Vereinbarungen die Weiterentwicklung oder Wartung der Software ein, so sind die AuftraggeberInnen berechtigt, die hinterlegten Datenträger zu entnehmen und entweder ein sachkundiges Unternehmen mit den erforderlichen weiteren Arbeiten (Wartung, Fehlerbehebung, …) zu beauftragen oder diese selbst durchzuführen.

Dabei ist zu beachten:

- Der Datenträger muss die Software in den ursprünglichen Programmiersprachen zum Zeitpunkt der Installation einschließlich aller seitherigen Änderungen enthalten.
- Der Datenträger muss die in maschinenlesbarer Form vorliegende Dokumentation enthalten.
- Es ist eine Aufstellung der versiegelt hinterlegten Gegenstände sowie eine Anweisung über die Handhabung des Datenträgers und die Installation der Software beizulegen.
- Die Hinterlegung muss bei jeder Lieferung einer neuen Version wiederholt werden, auf die Aktualität aller Komponenten sowie der Dokumentation ist zu achten.

Ein Vorschlag zur Formulierung einer entsprechenden vertraglichen Vereinbarung findet sich in den Allgemeinen Vertragsbedingungen der Republik Österreich für IT-Leistungen [AVB-IT] (siehe B.1 Sourcecodehinterlegung (Muster, aus AVB-IT)).

12.2.3 Dokumentation der Systemkonfiguration

Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation des vorhandenen IT-Systems. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf des IT-Systems.

Bei einem Netzbetrieb sind sowohl die physikalische Netzstruktur (vgl. 12.2.5 Dokumentation und Kennzeichnung der Verkabelung) als auch die logische Netzkonfiguration zu dokumentieren. Dazu gehören auch die Zugriffsrechte der einzelnen BenutzerInnen (siehe 9.2.2 Einrichtung und Dokumentation der zugelassenen BenutzerInnen und Rechteprofile) und der Stand der Datensicherung.

Dabei ist zu beachten:

- Die Dokumentation muss aktuell und verständlich sein, damit auch VertreterInnen die Administration jederzeit weiterführen können. Dies gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.
- Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch von Sicherheitsfunktionen) maßgeblich verändert werden.
- Um das Vertrauen in Betriebssysteme zu sichern, ist generell eine so genannte Vertrauenseinstellung im Zuge der Neuinstallation/-konfiguration vorzunehmen. Speziell im Bundesbereich ist gemäß [IKTB-170902-7] eine definierte sichere Initialkonfiguration zu verwenden. Deren Anwendung ist allerdings auch generell zu empfehlen. Eine entsprechend dokumentierte Initialkonfiguration wird im Rahmen des Online-Angebotes des Chief Information Office des Bundes zur Verfügung stehen. In diesem Zusammenhang: siehe auch 9.5.1 Sichere Initialkonfiguration und Zertifikatsgrundeinstellung.
- Die Unterlagen sind gesichert aufzubewahren, so dass ihre Verfügbarkeit im Bedarfsfall gewährleistet ist.

12.2.4 Dokumentation der Datensicherung

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat (vgl. 12.4 Datensicherung).

Zur Gewährleistung einer ordnungsgemäßen und funktionierenden Datensicherung ist eine Dokumentation erforderlich, die für jedes IT-System zumindest folgendes umfassen soll:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise, die sachverständigen Dritten eine Wiederherstellung eines Datensicherungsbestandes erlaubt. Auch hier muss eine Beschreibung der erforderlichen Hard- und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

12.2.5 Dokumentation und Kennzeichnung der Verkabelung

Für Wartung, Fehlersuche, Instandsetzung und für erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eindeutige Kennzeichnung aller Kabel erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit.

In dieser Dokumentation (auch Bestandsplan genannt) sind **alle** das Netz betreffenden Sachverhalte aufzunehmen:

- genauer Kabeltyp,
- nutzungsorientierte Kabelkennzeichnung,
- Standorte von zentralen Knoten und Verteilern mit genauen Bezeichnungen,
- genaue Führung von Kabeln und Trassen in der Liegenschaft (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- Trassendimensionierung und -belegung,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen NetzteilnehmerInnen,
- technische Daten von Anschlusspunkten,
- Gefahrenpunkte,
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen, andere Informationen können in Tabellenform geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten am Netz denjenigen rechtzeitig und vollständig bekannt werden, die die Dokumentation führen. Es ist z. B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Personen abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff darauf zu regeln.

Vgl. dazu auch 11.4.1 Lagepläne der Versorgungsleitungen.

12.2.6 Neutrale Dokumentation in den Verteilern

In jedem Verteiler sollte sich eine Dokumentation befinden, die den aktuellen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten. Nur bestehende und genutzte Verbindungen sind darin aufzuführen. Es sollen, soweit nicht ausdrücklich vorgeschrieben (z. B. für Brandmeldeleitungen) keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisionsdokumentation aufzuführen.

Es ist auf Aktualität, Vollständigkeit und Korrektheit dieser Information zu achten.

12.3 Schutz vor Schadprogrammen und Schadfunktionen

Computerviren (im Rahmen dieses Handbuchs der Einfachheit halber als Viren bzw. generell Schadprogramme bezeichnet) gehören zu den „Programmen mit Schadensfunktionen“ („maliziöse Software“). Dies sind Programme, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Damit verursachen sie zusätzliche Arbeit und Kosten und haben einen negativen Einfluss auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Programmen.

Zu den Programmen mit Schadensfunktionen gehören:

- Viren: Nichtselbstständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch von den AnwenderInnen nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen.
- Ransomware: Spezielle Form von Schadsoftware, die darauf ausgerichtet ist, Dateien bzw. Speicher zu verschlüsseln und somit unbrauchbar zu machen und in weiterer Folge für die Wiederherstellung Lösegeld (engl. „ransom“) zu erpressen.
- Trojanische Pferde: Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren.
- Logische Bomben: Programme, deren Schadensfunktion von einer logischen Bedingung gesteuert wird, beispielsweise dem Datum oder einer bestimmten Eingabe.

- Würmer: Selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten.

Eine Kategorisierung von derzeit auftretender Schadsoftware in nur eine dieser Formen ist üblicherweise nichtmehr zielführend, da diese meist mehrere verschiedene Fähigkeiten in sich vereinen.

Verbreitung:
Während früher Viren meist durch den Austausch „verseuchter“ Datenträger verbreitet wurden, ist heutzutage die Übertragung über Internet bzw. E-Mail der vorherrschende Verbreitungsweg. Bei den meisten über E-Mail verbreiteten „Viren“ handelt es sich eigentlich um Würmer, die - unabhängig von der eigentlichen Schadensfunktion - schon durch ihr massenhaftes Auftreten und ihre rasante Verbreitung großes Aufsehen erregen und zu hohen Schäden führen.

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer, die zur Vereinfachung im Folgenden generell als „Viren“ bezeichnet werden. Die angeführten Maßnahmen sind großteils auch gegen andere Arten von Software mit Schadensfunktion, wie z. B. Trojanische Pferde anwendbar.

12.3.1 Erstellung eines Virenschutzkonzepts

Um für ein komplexes IT-System oder eine gesamte Organisation einen effektiven Virenschutz zu erreichen, ist ein mehrstufiges Schutzkonzept erforderlich, bei dem in jeder Stufe angemessene und aufeinander abgestimmte Schutzmaßnahmen realisiert werden.

Schutzmaßnahmen sind zu treffen:

- auf Ebene der Firewall
- auf Server-Ebene
- auf Client-Ebene

Neben den technischen Schutzmaßnahmen sind auch organisatorische und personelle Maßnahmen erforderlich, um einem Virenbefall so weit wie möglich vorzubeugen, bzw. im Falle eines Virenbefalls den Schaden möglichst zu begrenzen.

Die nachfolgenden Maßnahmen geben eine Reihe von generellen Empfehlungen zum Virenschutz, die an die Erfordernisse der betroffenen Institution anzupassen sind. Je mehr bzw. je exakter die Empfehlungen umgesetzt werden, desto geringer wird das allgemeine Risiko. Allerdings können ggf. bestimmte (auch notwendige/ vorgesehene) Funktionen nicht mehr oder zumindest weniger produktiv durchgeführt werden. Die anzuwendenden Maßnahmen sind daher vor dem Hintergrund des Gesamtsystems und der jeweils gültigen Policy vorzuschreiben. Für die Effizienz des Virenschutzkonzeptes sind dabei nicht nur die ausgewählten Maßnahmen selbst von Bedeutung, sondern auch die Abstimmung dieser Maßnahmen aufeinander.

12.3.2 Generelle Maßnahmen zur Vorbeugung gegen Virenbefall

Die nachfolgend angeführten Maßnahmen dienen einer Vorbeugung gegen Virenbefall bzw. einer Verringerung des Schadens im Falle eines Befalls.

- Regelmäßige Durchführung einer Datensicherung (vgl. 12.4.1 Regelmäßige Datensicherung).
- Sichere Aufbewahrung der Sicherheitskopien von Datenträgern (vgl. 12.4.5 Geeignete Aufbewahrung der Backup-Datenträger).
- Setzen eines Schreibschutzes bzw. Nutzung von nur einmal beschreibbaren Medien bei allen Datenträgern, auf die nicht geschrieben werden muss (gilt insbesondere für Datenträger, die Programme beinhalten) und bei allen ausgehenden Datenträgern.
- Überprüfung aller ein- und ausgehenden Datenträger (vgl. auch 8.3.3 Datenträgeraustausch).
- Überprüfung aller vorinstallierten Neugeräte und gewarteten Geräte.
- Überprüfung aller ein- und ausgehenden Dateien über externe Netzwerke (E-Mails, Internet) (s. u.).
- Als vorbeugende Maßnahme gegen Virenbefall empfiehlt es sich, in der Boot-Reihenfolge die Systemfestplatte an erster Stelle einzustellen bzw. das Booten von externen Datenträgern (DVD, USB-Stick etc.) ganz zu unterbinden.
- Die Unterteilung der Festplatte in mehrere Partitionen kann die Rekonstruktion von Daten nach einem Virus-Schaden erleichtern (Anmerkung: Dies gilt auch bei einem Headcrash).
- Es sollten nur vertrauenswürdige Programme zugelassen sein, die auch über entsprechende Sicherheitsfunktionen verfügen. Dies gilt in besonderem Maße für E-Mail-Programme. „Private“ Insellösungen auf einzelnen Arbeitsplatzrechnern sollten nicht zugelassen werden, um die Sicherheit des Gesamtsystems nicht zu gefährden.
- Für Probleme sollten zentrale Ansprechpartner (E-Mail-Adresse, Telefonnummer) benannt werden.

12.3.3 Empfohlene Virenschutzmaßnahmen auf Firewall-Ebene

Viele Schadfunktionen (Nachladen von Code aus dem Internet; Übermittlung von vertraulichen Informationen aus dem geschützten Netz) benötigen definierte Verbindungswege in das Internet (Ports, Adressen), um ihre Wirkung entfalten zu können. Daher ist durch eine restriktive Politik bei den Filterregeln der Firewalls eine wesentliche Erhöhung der Sicherheit erreichbar.

Gateways bieten meist auch Möglichkeiten ohne teure Zusatzprodukte Maßnahmen zu setzen, die der Verbreitung von Schadprogrammen entgegenwirken. Dabei können Dateitypen (z. B. *.VBS, *.WSH, *.BAT, *.EXE), die im täglichen Arbeitsablauf nicht als Anhänge von E-Mails vorkommen, gleich zentral blockiert werden.

Der Einsatz spezieller Rechner, die den Datenverkehr auf Viren und auch den Inhalt der E-Mails scannen können, ist in Form einer erweiterten Gatewayfunktionalität oder der Einbindung über eigene Protokolle (z. B. Content Vectoring Protocol) möglich. Dabei können E-Mails mittels Virenscanner verschiedener Hersteller überprüft werden und - sogar vor dem Vorliegen der neuen Virensignaturen - durch das Filtern entsprechender Textbegriffe die Ausbreitung neuer Schadsoftware gestoppt werden.

Sollten Informationen blockiert werden, empfiehlt es sich, den AbsenderInnen einer solchen E-Mail eine automatisierte Nachricht zukommen zu lassen, dass ihre E-Mails nicht zugestellt werden konnten oder (besser) einen SMTP-Error zu erzeugen und somit den zustellenden Server über die Nichtzustellung zu informieren.

12.3.4 Empfohlene Virenschutzmaßnahmen auf Server-Ebene

Auf E-Mail-Servern und allen Servern, die zum Datenaustausch genutzt werden, sollten Virenschutzprogramme zur zentralen Überprüfung des E-Mail-Verkehrs und der ausgetauschten Dateien installiert werden (vgl. dazu auch 12.3.8 Auswahl und Einsatz von Virenschutzprogrammen).

Dabei ist auf eine regelmäßige Aktualisierung der eingesetzten Programme zu achten.

12.3.5 Empfohlene Virenschutzmaßnahmen auf Client-Ebene und Einzelplatzrechnern

- Aktivierung aller vorhandenen Sicherheitsfunktionen des Rechners (Passwort-Schutz, Bildschirmschoner mit Passwort etc.), damit während der Abwesenheit der berechtigten BenutzerInnen Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.
- Einsatz eines aktuellen Virenschutzprogrammes mit aktuellen Signaturdateien, das im Hintergrund läuft (resident) und bei bekannten Viren Alarm schlägt. (Auch wenn am E-Mail-Server bereits ein Virenschutzprogramm zum Einsatz kommt, empfiehlt sich die Installation dezentraler Virenschutzprogramme, um beispielsweise auch Schutz bei verschlüsselter Kommunikation zu erreichen.)
- Aktivierung der Anzeige aller Dateitypen im Browser bzw. E-Mail-Programm.
- Aktivierung des Makrovirenschutzes von Anwendungsprogrammen (MS Word, Excel, Powerpoint etc.) und Beachtung von Warnmeldungen.

- Sofern möglich: Wahl der höchsten Stufen in den Sicherheitseinstellungen von Internet-Browsern (Deaktivieren von aktiven Inhalten und Skript-Sprachen aus unbekannten Quellen etc.).
- Keine Nutzung von Applikationsverknüpfungen für Anwendungen mit potenziell aktivem Code (MS-Office) im Browser, keine Aktivierung von Anwendungen über Internet.
- Die Ausführung von aktiven Inhalten in E-Mail-Programmen immer unterbinden (entsprechende Optionen setzen).
- Durch den Einsatz eines Firewall-Produkts auf den Einzelplatzrechnern (Personal Firewalls), die regeln, welche Programme auf das Internet zugreifen dürfen, kann der Schadsoftware ebenfalls gezielt entgegengewirkt werden. Dadurch wird die zentrale Firewall, die keine Informationen über die aufrufenden Programme hat, wirkungsvoll ergänzt (vgl. 13.1.15 Sicherer Betrieb einer Firewall).

12.3.6 Vermeidung bzw. Erkennung von Viren durch die BenutzerInnen

Die Sensibilisierung der EndanwenderInnen für die Virenproblematik stellt eine wichtige Komponente beim Schutz gegen Viren dar. Daher sollte in Schulungen regelmäßig auf die Gefahr von Viren, die Möglichkeiten zu ihrer Erkennung und Vermeidung sowie die notwendigen Handlungsanweisungen im Falle eines (vermuteten) Virenbefalls hingewiesen werden. Auch laufende Informationen zu diesem Thema, etwa über das Intranet oder in Form interner Publikationen, sind empfehlenswert.

Erkennen potenzieller Gefahren bei eingehender E-Mail und Abwehrmaßnahmen:

- Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen AbsenderInnen prüfen, ob der Text der Nachricht auch zu den AbsenderInnen passt (englischer Text von deutscher Partnerin bzw. deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.
- Vorsicht bei mehreren E-Mails mit gleichlautendem Betreff.
- Kein „Doppelklick“ bei ausführbaren Programmen (*.COM, *.EXE) oder Script-Sprachen (*.VBS, *.BAT etc.) (sofern sie nicht bereits auf Firewall-Ebene gefiltert wurden).
- Vorsicht auch bei Dateien von Anwendungsprogrammen (Office etc.) sowie Bildschirmschonern (*.SCR).
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.

- Nur vertrauenswürdige E-Mail-Attachments öffnen (z. B. in letzter Konsequenz sogar nach telefonischer Absprache). Es ist zu beachten, dass die Art des Dateianhangs (Attachment) bei Sabotageangriffen oft getarnt ist und über ein Icon nicht sicher erkannt werden kann.
- Die Konfiguration der E-Mail-Clients sollte so eingestellt sein, dass Attachments nicht automatisch geöffnet werden. Außerdem sollten als E-Mail-Editor keine Programme mit der Funktionalität von Makrosprachen (z. B. MS Word) oder Scripts eingesetzt werden. Bei der Verwendung des HTML-Formates ist ebenfalls Vorsicht geboten.

Empfohlene Verhaltensregeln im Verdachtsfall:

Verdächtige E-Mails bzw. deren Attachments sollten auf keinen Fall von den EndanwenderInnen geöffnet werden.

Im Privatbereich und evtl. auch in Teilen des kommerziellen Bereiches wird ein sofortiges Löschen von offensichtlich unsinnigen oder irgendwie verdächtigen E-Mails empfehlenswert sein, um der Gefahr einer Vireninfektion zu begegnen. In Bereichen, wo dies entweder aufgrund gesetzlicher Vorschriften oder kommerzieller Überlegungen nicht möglich ist, ist dafür zu sorgen, dass verdächtige E-Mails in entsprechend sicherer Umgebung geöffnet und analysiert werden können. Dazu sind sog. „Quarantänebereiche“ einzurichten, in denen die E-Mails von Spezialistinnen bzw. Spezialisten untersucht und weiterbehandelt werden können. BenutzerInnen müssen wissen, wie sie diese SpezialistInnen erreichen oder E-Mails an solche Bereiche weiterleiten können.

Maßnahmen bei ausgehender E-Mail:

Durch Beachtung der nachfolgenden Maßnahmen kann die Gefahr reduziert werden, dass EndanwenderInnen unabsichtlich Viren verteilen:

- Vermeidung aktiver Inhalte in E-Mails.
- Keine unnötigen E-Mails mit Scherzprogrammen und ähnlichem versenden, da diese evtl. einen Computervirus enthalten können.
- Keinen Aufforderungen zur Weiterleitung von Warnungen, E-Mails oder Anhängen an Freundinnen bzw. Freunde, Bekannte oder Kollegen folgen, sondern direkt nur an die CISOs senden. Es handelt sich nämlich meist um irritierende und belästigende E-Mails mit Falschmeldungen (Hoax oder „elektronische Ente“, Kettenbrief).
- Gelegentlich prüfen, ob E-Mails im Postausgang stehen, die nicht selbst verfasst wurden.

Verhalten bei Downloads aus dem Internet:

Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Viren und „Trojanische Pferde“ dar, die verwendet werden um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen. Es muss darauf hingewiesen werden, dass auch Dateien von Office- und anderen Anwendungsprogrammen (Text-, Tabellen- und Präsentationsdateien, PDF etc.) Makroviren bzw. Scripts mit Schadensfunktion enthalten können.

- Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten der HerstellerInnen. Private Homepages, die bei anonymen Webspace-Providern eingerichtet werden, stellen hierbei eine besondere Gefahr dar.
- Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden. Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.
- Mit einem aktuellen Virenschutzprogramm sollten vor der Installation die Dateien immer überprüft werden.
- Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.

12.3.7 Erstellung von Notfallplänen im Fall von Vireninfektionen

- Die Informationswege für Notfälle sind zu planen, die zuständigen Funktionen oder Personen zu definieren, Ausweichwege für die Kommunikation und Vertretungsregeln festzulegen.
- Je nach vorliegendem Schadprogramm sind Verfahren zur differenzierten E-Mail-Filterung (z. B. Größenbeschränkung, keine Attachments, nur Posteingang, Filterung von bestimmten Betreffen) vorzubereiten und auch zu testen. Da E-Mail mittlerweile das zentrale Informationsmedium geworden ist, dürfen diese Systeme allenfalls kurzzeitig deaktiviert werden, damit nach wie vor Warnungen möglich sind.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die Updates der Virenschutzprogramme möglichst rasch auf Servern, Gateways und Clients eingestellt werden. Die entsprechenden Verteilwege und Maßnahmen sind vorzubereiten und selbstverständlich auch regelmäßig zu testen.
- Sollten durch einen neuen Virus die üblichen Informationswege nicht verfügbar sein, sind alternative Verfahren zur zeitnahen Warnung vorzusehen (z. B. notfalls auch durch SMS, Telefon- und Informationsdisplays, Lautsprecherdurchsagen).

- Für den Notfall sind Backup- und Restore-Strategien zu erarbeiten, die festlegen, welche Rechner in welcher Reihenfolge in betriebsbereiten Zustand zu bringen sind, damit in kürzester Zeit eine, wenn auch eingeschränkte, Funktionsfähigkeit hergestellt werden kann.

12.3.8 Auswahl und Einsatz von Virenschutzprogrammen

Zum Schutz vor Viren können unterschiedliche Wirkprinzipien genutzt werden.

Programme, die Speichermedien nach bekannten Viren durchsuchen, haben sich in der Vergangenheit als effektivstes und wirksamstes Mittel in der Virenbekämpfung erwiesen. Von Vorteil ist, dass neu erhaltene Software oder Datenträger schon vor dem ersten Einsatz geprüft werden können. Man kann daher eine Infektion mit bekannten Viren grundsätzlich vermeiden. Ein weiterer Vorteil ist, dass man durch das Virenschutzprogramm eine genauere Information über den jeweils entdeckten Virus erhält. Die bekannten Viren sind durch SpezialistInnen analysiert worden, so dass man weiß, ob und welche Schadensfunktionen vorhanden sind. Ein gutes Virenschutzprogramm muss daher nicht nur in der Lage sein, viele Viren zu finden, sondern sie auch möglichst exakt zu identifizieren. Zahlreiche Programme bieten auch die Möglichkeit einer Entfernung gefundener Viren an. Hierbei ist zu beachten, dass die Qualität dieser Entfernungsroutinen sehr unterschiedlich ist. Wenn immer möglich, sollten mit der Entfernung SpezialistInnen betraut werden.

Zu beachten ist, dass Virenschutzprogramme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Erstellungszeitpunkt bekannten Viren berücksichtigen, neu hinzugekommene jedoch meist nicht erkennen können. Daher ist eine regelmäßige Aktualisierung des Virenschutzprogramms erforderlich.

Ebenso wie andere Programme können sie durch Aufruf (transient) oder im Hintergrund (resident) genutzt werden. Die Betriebsart des Virenschutzprogramms hat entscheidenden Einfluss auf die Akzeptanz bei den AnwenderInnen und damit auf die tatsächlich erreichte Schutzfunktion.

Beim transienten Betrieb wird das Programm aufgerufen, durchsucht die eingestellten Teile des Computers, beendet seine Arbeit danach und macht den Speicher wieder frei. Meist lösen die AnwenderInnen den Aufruf aus.

Beim residenten Betrieb wird das Virenschutzprogramm beim Start des Rechners in den Speicher geladen und verbleibt dort aktiv bis zum Ausschalten. Es verrichtet seine Tätigkeit, ohne dass die AnwenderInnen dabei mitwirken, sie können inzwischen ihre eigentliche Arbeit, z. B. das Schreiben von Texten, ausführen.

Eine weitere präventive Maßnahme ist der Einsatz von **Checksummen-Prüfprogrammen**. Hierbei werden zum Schutz vor Veränderung von den zu prüfenden Dateien oder Systembereichen (z. B. Boot- und Partition-Sektor) Prüfsummen berechnet, die regelmäßig kontrolliert werden. Auf diese Weise können nicht nur Verseuchungen mit bisher unbekannten Viren erkannt werden, sondern auch andere unberechtigte Veränderungen an Dateien.

Im Wesentlichen sollte ein Virenschutzprogramm folgende Eigenschaften erfüllen:

- Der Umfang der erkannten Viren sollte möglichst groß sein und dem aktuell bekannten Bestand entsprechen, insbesondere müssen alle sehr stark verbreiteten Viren erkannt werden.
- Eine ständige Aktualisierung bezüglich neuer Viren muss vom Hersteller sichergestellt sein.
- Das Programm sollte Viren auch in komprimierter Form finden, wobei alle gängigen Komprimierungsfunktionen (wie z. B. PKZIP) unterstützt werden sollten.
- Gefundene Viren müssen mit einer vollständigen Pfad-Angabe angezeigt werden.
- Das Programm muss seine eigene Virenfreiheit feststellen, bevor die Suchfunktion ausgeführt wird.
- Nach Möglichkeit muss das Produkt als residentes Programm eine permanente Virenkontrolle ermöglichen.
- Sinnvoll ist eine Funktionalität, die es erlaubt, erkannte Viren zu entfernen, ohne weitere Schäden an Programmen oder Daten zu verursachen.
- Das Programm sollte über eine Protokollierungsfunktion verfügen, die folgende Daten festhält:
    - Versionsstand des Programms,
    - Datum und Uhrzeit der Überprüfung,
    - Angabe aller benutzten Parameter,
    - Prüfergebnis mit Prüfumfang,
    - Anzahl und Identifikation der Dateien und Objekte, die nicht geprüft werden konnten.
- Das Programm sollte eine Warnung ausgeben, wenn es feststellt, dass es offensichtlich nicht aktualisiert wurde.
- Das Programm sollte eine Liste der erkennbaren Viren und ihre Beschreibung beinhalten. Darüber hinaus sind jeweils Beschreibungen von Sofortmaßnahmen und Maßnahmen zum Entfernen des Virus anzugeben.

12.3.9 Verhaltensregeln bei Auftreten eines Virus

Gibt es Anzeichen, dass ein Rechner von einem Virus befallen ist (z. B. Programmdateien werden länger, unerklärliches Systemverhalten, nicht auffindbare Dateien, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde), so sind zur Feststellung des Virus und zur anschließenden Beseitigung folgende Schritte durchzuführen.

Grundregel: Falls möglich, sollten fachkundige BetreuerInnen (AdministratorInnen, Bereichs-IT-Sicherheitsverantwortliche, Helpdesk) zu Hilfe geholt werden.

Falls dies nicht möglich ist, sollten folgende Schritte durchgeführt werden:

1. Beenden der laufenden Programme und Abschalten des Rechners.
2. Booten des Rechners von einer einwandfreien, geprüften Notfall-CD (evtl. vorher Boot-Reihenfolge im BIOS-Setup ändern, siehe 12.3.2 Generelle Maßnahmen zur Vorbeugung gegen Virenbefall).
3. Überprüfen des Rechners mit einem aktuellen Virenschutzprogramm um festzustellen, ob tatsächlich ein Virus aufgetreten ist und um welchen Virus es sich ggf. handelt.
4. Entfernen des Virus abhängig vom jeweiligen Virustyp.
5. Erneute Überprüfung der Festplatte mit dem Virensuchprogramm.
6. Untersuchung aller anderen Datenträger (USB-Sticks, Wechselplatten etc.) auf Virenbefall und Entfernung eventuell vorhandener Viren.
7. Es sollte versucht werden, die Quelle der Vireninfektion festzustellen. Ist die Quelle auf Originaldatenträger zurückzuführen, dann sollte der Hersteller informiert werden. Liegt die Quelle in Dateien oder E-Mail, so sind die ErstellerInnen der Datei zu unterrichten.
8. Warnung an andere IT-BenutzerInnen, wenn ein Datenaustausch vom infizierten Rechner erfolgte.

Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme (vgl. 12.4.6 Sicherungskopie der eingesetzten Software) zu rekonstruieren.

Anschließend ist das wiederhergestellte System noch einmal auf Schadsoftware zu überprüfen.

12.3.10 Warnsystem für Computerviren – Aktualisierung von Virenschutzprogrammen

Im Zusammenhang mit Computerviren ist die permanente Aktualität des verwendeten Virenschutzprogrammes von größter Wichtigkeit. Bereits bei der Beschaffung von Virenschutzprogrammen ist daher für die Aktualisierbarkeit und die Versorgung von entsprechenden Updates durch den Hersteller Sorge zu tragen. Darüber hinaus sind die Verantwortlichkeiten für die regelmäßig durchzuführenden Aktualisierungen innerhalb der Organisation zu definieren.

Neben der Aktualisierung der eingesetzten Software ist auch die Information über neue Computerviren, sowie Informationen über empfohlene aktive und passive Gegenmaßnahmen, besonders wichtig. Dabei genügt es oft nicht, sich nur auf die periodischen Updates des Virenschutzprogrammherstellers zu verlassen. Im Bereich der öffentlichen Verwaltung wurde ein eigenes Government Computer Emergency Response Team (GovCERT.AT) eingerichtet. Dieses wird in Kooperation mit CERT.at zur Behandlung beziehungsweise Verhinderung von Sicherheitsvorfällen im Bereich der Informations- und Kommunikationstechnologien betrieben. Dabei wird u. a. mit einem Warnsystem für Computerviren und sonstigen schädigenden Inhalten eine Informationsbasis und ein Verteilsystem für derartige Informationen geschaffen, welches den geeigneten Stellen der öffentlichen Verwaltung und der Wirtschaft zur Verfügung steht.

12.3.11 Schutz vor aktiven Inhalten

Eines der größten Probleme bei der Konzeption eines Sicherheitsgateways (Firewall) ist die Behandlung der Probleme, die durch die Übertragung aktiver Inhalte zu den Rechnern im zu schützenden Netz entstehen. Derzeit existieren noch keine brauchbaren Programme, die eine ähnlich wirksame Erkennung von Schadfunktionen in ActiveX-Controls, Java-Applets oder Scripting-Programmen ermöglichen, wie sie im Bereich der Computerviren möglich ist.

Mittlerweile sind die meisten dieser Technologien Auslaufmodelle oder werden generell nichtmehr unterstützt. ActiveX-Controls, Java-Applets, Flash, Silverlight und ähnliche können getrost deaktiviert oder deinstalliert werden, sofern sie überhaupt noch von Browsern oder anderen Programmen unterstützt werden. Einzig Scripting-Programme sind noch eine relevante Bedrohung aus dem Bereich der aktiven Inhalte. Ein Schutz vor aktiven Inhalten ist jedoch unabhängig von der aktuellen Bedrohungslage zu implementieren.

Die Größe der Gefährdung, die von aktiven Inhalten für die Rechner im zu schützenden Netz ausgeht, lässt sich anhand des folgenden Beispiels darstellen: Ein Java-Applet bzw. der Browser darf gemäß der Java-Spezifikationen eine Netzverbindung zu dem Server aufbauen, von dem es geladen worden ist. Diese zur Zeit noch recht wenig benutzte Möglichkeit ist eine zentrale Voraussetzung, wenn Netz-Computer (NC) oder ähnliches eingesetzt werden sollen, die auch ohne spezielle Initiierung durch den/die AnwenderIn Programme vom Server laden müssen. Um diese Eigenschaft trotz der Verwendung eines Paketfilters vollständig

unterstützen zu können, müssen sehr viel mehr Ports freigeschaltet werden oder es muss ein dynamischer Paketfilter eingesetzt werden. Ist das der Fall, können Java-Applets verwendet werden, um kaum zu kontrollierende IP-Verbindungen aufbauen zu können.
Die Kontrolle aktiver Inhalte kann auf verschiedene Weise geschehen:

1. Zentrale Filterung der aktiven Inhalte auf der Firewall
   Sämtliche als schädlich eingestuften Inhalte werden von einer Komponente der Firewall gefiltert, so dass keine potenziell schädlichen Programme mehr auf den Client-Rechnern eintreffen. Aktive Inhalte werden über spezielle Tags innerhalb einer HTML-Seite eingebunden. In der Regel werden aktive Inhalte anhand der entsprechenden Tags aus einer HTML-Seite erkannt und gelöscht, oder sie werden durch einen Textbaustein ersetzt, der dem Anwender einen Hinweis über die Tatsache der Filterung gibt. Das Problem besteht dabei darin, dass wegen der komplexen Möglichkeiten der aktuellen HTML-Spezifikation oft nicht alle zu löschenden Tags von den Sicherheitsproxies erkannt werden. Weiters ist problematisch, dass beispielsweise Java-Applets nicht notwendigerweise als Datei mit der Endung .class verschickt werden müssen. Stattdessen können auch komprimierte Dateien eingesetzt werden, die z. B. die Endung .jar (Java-Archive) haben. Das bedeutet, dass ein Java-Filter auch alle von den verwendeten Browsern unterstützten Dateiendungen für Java-Dateien kennen muss. Zusätzliches Schadenspotenzial resultiert auch aus der Möglichkeit, JavaScript aus Java heraus auszuführen. Ähnliche Probleme existieren im Zusammenhang mit Flash-Objekten, .NET Assemblies und anderen aktiven Inhalten. Es sollte unbedingt beachtet werden, dass auch aktive Inhalte außerhalb von Webseiten gefiltert werden müssen, beispielsweise in HTML-E-Mails.
2. Dezentrale Abwehr auf den angeschlossenen Clients
   Die Ausführung aktiver Inhalte sollte normalerweise durch entsprechende Einstellungen im Browser unterbunden werden. Die Umsetzung einer Whitelist-Strategie für aktive Inhalte wird von verschiedenen Browsern in unterschiedlicher Weise und mehr oder weniger gut unterstützt (Beispiel: Browser-Profile bei Mozilla Firefox). Idealerweise sollte ein Browser die Möglichkeit bieten, die Ausführung bestimmter Typen aktiver Inhalte getrennt für einzelne Server oder Domains freigeben oder verbieten zu können. Dabei ist allerdings zu beachten, dass es aufgrund von Schwachstellen in den Browsern Angreifern möglich sein kann, entsprechende Einschränkungen zu umgehen. Java-Applets, Active-X Objekte und mit Einschränkungen auch Javascript können mit einer digitalen Signatur versehen werden. Die Signatur dient dazu, die Integrität und Authentizität des jeweiligen aktiven Inhalts zu schützen. Werden ausschließlich signierte aktive Inhalte zugelassen, so bietet dies eine erhöhte Sicherheit vor Schadfunktionen. Diese Sicherheit ist jedoch nur indirekt, da der Nutzer auf die Vertrauenswürdigkeit der Signaturstelle, die in Zusammenarbeit mit dem Anbieter der aktiven Inhalte die Signatur erstellt, angewiesen ist. Selbst die vollständige Deaktivierung der Ausführung aktiver Inhalte bietet aber nur einen

begrenzten Schutz vor bösartigen aktiven Inhalten. Aufgrund der Vielzahl von Softwareschwachstellen in den Browsern können die Sicherheitseinstellungen umgangen werden, so dass der intendierte Schutz tatsächlich nicht oder nicht in vollem Umfang existiert.

3. Installation von Antivirensoftware und Personal Firewalls auf den Clients
   Antivirenprodukte können vor Viren, Makroviren und Trojanischen Pferden schützen, die durch aktive Inhalte automatisch heruntergeladen wurden. Sie bieten einen guten Schutz vor bereits bekannten Schadprogrammen. Personal Firewalls sind Programme, die auf dem Client-Rechner installiert werden und dort meist mehrere Funktionen wahrnehmen. Sie bieten meist neben der Funktion eines lokalen Paketfilters weitere Funktionen an. Beispielsweise bieten einige Personal Firewalls die Möglichkeit einer Überwachung anderer Programme, die versuchen eine Netz-Verbindung aufzubauen. Solche Verbindungsaufnahmen können dann meist entweder automatisch anhand festgelegter Regeln oder im Einzelfall vom Benutzer selbst erlaubt oder verboten werden. In einigen Fällen bieten sie auch sogenannte „Sandboxen“, die die Ausführung aktiver Inhalte kontrollieren und auf unbedenkliche Operationen beschränken können. Personal Firewalls bieten zusammen mit Antivirenprogrammen einen recht guten Schutz vor bösartigen aktiven Inhalten. Allerdings muss berücksichtigt werden, dass die richtige Konfiguration dieser Programme zusätzlichen Administrationsaufwand erfordert, und dass Personal Firewalls selbst Sicherheitslücken aufweisen können, die das System gefährden.

Bei allen drei Optionen ist eine Sensibilisierung der BenutzerInnen zusätzlich notwendig. Zudem muss sichergestellt werden, dass die Einstellungen auf den Clients bei allen unter Punkt 2 und 3 genannten Schutzvorkehrungen nicht versehentlich oder absichtlich von den BenutzerInnen deaktiviert oder umgangen werden können.

Die Entscheidung, wie mit aktiven Inhalten in Webseiten umgegangen wird, hängt in erster Linie vom Schutzbedarf der betreffenden Clients ab.

Die Entscheidung für eine bestimmte Vorgehensweise und die Gründe, die dafür ausschlaggebend waren, sollten nachvollziehbar dokumentiert werden.

Eine zu „liberale“ Einstellung oder gar eine generelle Freigabe aktiver Inhalte ist auch bei normalem Schutzbedarf nicht zu empfehlen. Die möglichen Schäden, die durch bösartige aktive Inhalte in Verbindung mit Schwachstellen in Webbrowsern oder im unterliegenden Betriebssystem entstehen können, sind dafür zu gravierend. Falls für bestimmte Anwendungen aktive Inhalte zwingend nötig sind, sollten sie nur für die betreffenden Server freigegeben werden.

Bei Neuentwicklungen browserbasierter Anwendungen oder bei einer Weiterentwicklung einer bestehenden Anwendung, die aktive Inhalte im Browser benötigt, sollte kritisch hinterfragt werden, ob die Verwendung der aktiven Inhalte wirklich notwendig ist. Oft lassen sich aktive Inhalte bei gleichwertiger Funktionalität durch serverseitig dynamisch erzeugte Webseiten ersetzen.

Empfehlungen für **normalen Schutzbedarf**:

- Deaktivierung aktiver Inhalte im Browser und Freischaltung nur für vertrauenswürdige Websites.
- Virenscanner auf dem Client.
- Eine Filterung aktiver Inhalte auf dem Sicherheitsgateway mit Freischaltung für vertrauenswürdige Websites (Whitelist).

Empfehlungen für **hohen Schutzbedarf** (zusätzlich zu den o. g. Empfehlungen für normalen Schutzbedarf):

- Filterung von Cookies (Whitelist).
- Die Kriterien, für welche Websites aktive Inhalte freigeschaltet werden, sollten deutlich restriktiver sein.
- Eine ergänzende Sicherheitsanalyse wird empfohlen, um sicher zu stellen, dass ein angemessenes Sicherheitsniveau erreicht wurde

12.3.12 Sicherer Aufruf ausführbarer Dateien

Ausführbare Dateien können direkt gestartet werden. Im Gegensatz hierzu können Anwendungsdaten, wie Textdateien, nur über ein entsprechendes Programm angesehen werden. Unter Windows sind ausführbare Dateien an ihrer Dateiendung (beispielsweise .exe, .com, .vbs, .bat, .cmd) und unter Unix oder Linux durch Dateirechte (x-Flag) erkennbar.

Es muss sichergestellt werden, dass nur freigegebene Versionen ausführbarer Dateien und keine eventuell eingebrachten modifizierten Versionen (insbesondere Trojanische Pferde) aufgerufen werden (siehe auch 14.1.7 Abnahme und Freigabe von Software).

AngreiferInnen könnten ausführbare Dateien soweit verändern, dass sie die Privilegien der BenutzerInnen erhalten, die die Datei ausführen. Um dies zu verhindern, dürfen ausführbare Dateien nur lesbar sein. Ein Schreibzugriff darf nur AdministratorInnen gestattet werden

Ausführbare Dateien, für die Schreibrechte benötigt werden, z. B. weil sie sich in der Entwicklung befinden, dürfen nur in separaten Bereichen verwendet werden. Dasselbe gilt für neue Software, die für einen späteren Einsatz auf einem Produktivsystem getestet werden soll. Hierfür können beispielsweise separate Testsysteme eingesetzt werden oder spezielle Benutzerkonten ohne weitere Privilegien. Nur so kann verhindert werden, dass diese Applikationen Schaden anrichten.

Auch bereits getestete Software kann die Sicherheit beeinträchtigen. Dies betrifft vor allem sehr komplexe Anwendungen wie zum Beispiel Webserver. Schon beim Start von Anwendungen muss sichergestellt werden, dass jeder Prozess nur so viele Rechte erhält, wie unbedingt notwendig sind. So kann bei einem erfolgreichen Angriff der eintretende Schaden begrenzt werden. Diese Dienste dürfen, wenn möglich, nicht mit Administratorrechten gestartet werden. Hierfür eignen sich ebenfalls Benutzerkonten mit eingeschränkten Privilegien. Über klare Trennungen von Rechten, unter Unix oder Linux beispielsweise durch chroot-Umgebungen, die den eintretenden Schaden begrenzen können, muss nachgedacht werden.

Im Weiteren muss sichergestellt werden, dass nur die gewünschte, freigegebene Version ausgeführt werden kann. AngreiferInnen könnten sonst eine modifizierte Datei mit dem selben Namen in ein Verzeichnis kopieren, auf das sie Schreibrechte haben. Wird beim Aufruf in den Verzeichnissen nach der Datei gesucht, könnte die modifizierte statt der gewünschten Datei ausgeführt werden.

Bei vielen Betriebssystemen werden die Verzeichnisse, in denen nach den ausführbaren Dateien gesucht werden soll, in der entsprechenden Reihenfolge in der PATH-Variable eingetragen. Die Anzahl der angegebenen Verzeichnisse sollte gering und überschaubar gehalten werden. Relative Verzeichnisangaben, die das jeweils aktuelle Arbeitsverzeichnis enthalten, dürfen als Angabe in der PATH-Variable nicht enthalten sein. Ausführbare Dateien sollen nur in dafür vorgesehenen Verzeichnissen gespeichert sein. In den in einer PATH-Variable enthaltenen Verzeichnissen darf nur der jeweilige Eigentümer Schreibrechte erhalten. Dies muss regelmäßig überprüft werden.

12.3.13 Vermeidung gefährlicher Dateiformate

E-Mail ist einer der wichtigsten Übertragungswege für Computerviren und -würmer. Eine rein textbasierte E-Mail ohne Anhänge ist dabei ungefährlich. Gefährlich wird es erst, wenn E-Mail-Anhänge ausgeführt werden oder die E-Mail HTML-basiert ist (siehe unten). Prinzipiell können E-Mails Anhänge in beliebiger Art und Menge beigefügt werden. Durch ein Zuviel an Anhängen kann die Verfügbarkeit eines E-Mail-Clients oder des E-Mail-Servers beeinträchtigt werden. Die größere Gefahr sind aber Anhänge, die ausführbaren Code enthalten und damit ungeahnte Nebeneffekte auslösen können.

Der E-Mail-Client sollte so eingestellt sein, dass Anhänge nicht versehentlich gestartet werden können, sondern das Programm vor der Ausführung warnt bzw. zumindest nachfragt, ob die Datei geöffnet werden soll. Das Betriebssystem bzw. der E-Mail-Client sollte außerdem so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltenen Programmcode, wie Makros oder Skripte, nicht ausführen.

Vor dem Absenden einer E-Mail sollte sich jeder überlegen, ob es wirklich nötig ist, ein Attachment anzuhängen, oder ob die Informationen nicht genauso gut als Text in die E-Mail direkt eingefügt werden kann. Ansonsten sollten Dateien in möglichst „ungefährlichen“ Formaten weitergegeben werden. Wenn sich die Versendung von Dateien in „gefährlichen“ Formaten nicht vermeiden lässt, sollte überlegt werden, den Empfänger mit einer kurzen E-Mail darauf hinzuweisen, dass als nächstes eine E-Mail mit solchen Attachments zu erwarten ist.

Für den Umgang mit Dateiformaten, die als potenziell problematisch eingeschätzt werden, können verschiedene Regelungen getroffen werden. Wichtig ist aber auf jeden Fall, dass alle Betroffenen sich der Problematik bewusst sind und entsprechend vorsichtig mit diesen Dateiformaten umgehen.

Die restriktivste Form ist es, das Öffnen aller als problematisch eingestuften Dateiformate zu verbieten bzw. diese am E-Mail-Gateway herauszufiltern. Dies führt allerdings erfahrungsgemäß zu großen Akzeptanzproblemen seitens der KundInnen und der MitarbeiterInnen. Besser ist es im Allgemeinen, einerseits die MitarbeiterInnen für die Problematik zu sensibilisieren und zum Mitdenken anzuregen und sie andererseits technisch zu unterstützen, indem die Gefährdungspotenziale durch entsprechende Konfiguration und Sicherheitswerkzeuge minimiert werden.

Im Folgenden werden einige Einschätzungen verschiedener Dateiformate gegeben. Diese können sich allerdings jederzeit ändern, wenn z. B. ein Hersteller seinem Produkt neue Features hinzufügt, die ungeplante Nebenwirkungen haben, bzw. SoftwareanalystInnen solche Nebenwirkungen herausfinden.

- Als weitgehend harmlos gelten bisher ASCII-, GIF-, JPEG-formatierte Dateien.
- Als möglicherweise gefährlich sollten die folgenden Dateiformate behandelt werden: alle Dateiformate von Office-Paketen wie Microsoft Office, LibreOffice oder OpenOffice.org mit integrierter Makrosprache, z. B. Word, Excel, Powerpoint (.DOC, .XLS, .PPT, SDW, SXW usw.). Besonders kritisch sind alle ausführbaren Programme (wie .COM, .EXE, .PIF) oder Skript-Sprachen (.VBS, .JS, .BAT unter Windows, ebenso wie Perl- oder Shellskripte unter Unix), Registrierungsdateien (.REG) sowie Bildschirmschoner (.SCR). Vorsichtshalber sollte für alle diese Dateitypen eine „ungefährliche“ Standardapplikation festgelegt werden, mit der diese zwar geöffnet werden, innerhalb deren aber eventuelle Computerviren keinen Schaden auslösen können. Beispielsweise sollten Dateitypen wie *.VBS, *.JS oder *.BAT grundsätzlich mit einem einfachen, nicht makrofähigen Texteditor geöffnet werden. Windows-Betriebssysteme sollten außerdem so konfiguriert sein, dass bei Registrierungsdateien (.REG) als Standardvorgang „Bearbeiten“ statt „Zusammenführen“ eingestellt ist. Dadurch wird die Datei zunächst in einem Editor dargestellt und nicht der Registrierungsdatenbank hinzugefügt, wenn sie aktiviert wird.

- Mit Zusatzmaßnahmen als vertretbar angesehen werden können: HTML, wenn ein JavaScript-Filter oder andere Sicherheitsvorkehrungen eingesetzt werden, RTF (mit COM-Object-Filter), ZIP (hier sollten die BenutzerInnen allerdings gewarnt werden, dass die enthaltenen Dateien problematisch sein können), PDF (dabei ist darauf zu achten, dass z. B. die Software „PDF Reader“ auf dem Endgerät als Standard installiert ist und nicht „Adobe Acrobat“).

Immer mehr E-Mails sind heutzutage auch HTML-formatiert. Dies ist einerseits oft lästig, weil nicht alle E-Mail-Clients dieses Format anzeigen können. Andererseits kann dies aber auch dazu führen, dass bereits bei der Anzeige solcher E-Mails auf dem Client ungewollte Aktionen ausgelöst werden, da HTML-Mails eingebetteten JavaScript- oder VisualBasic-Skript-Code enthalten können.

Durch Kombination verschiedener Sicherheitslücken in E-Mail-Clients und Browsern ist es in der Vergangenheit immer wieder zu Sicherheitsproblemen mit HTML-formatierten E-Mails gekommen.

Generell sollten möglichst keine HTML-formatierten E-Mails oder solche mit aktiven Inhalten versendet werden. Außerdem sollte die Möglichkeit überprüft werden, in eingehenden E-Mails enthaltene aktive Inhalte herauszufiltern, beispielsweise an der Firewall.

Weiters sollten E-Mail-Clients gewählt werden, bei denen HTML-formatierte E-Mails als solche zu erkennen sind, damit die BenutzerInnen diese nicht unbewusst öffnen.

Generell sollte eine Vorgabe innerhalb einer Organisation zum Umgang mit HTML-formatierten E-Mails erstellt werden. Beim Empfang von HTML-formatierten E-Mails sollte festgelegt werden, ob diese

- unverändert an die BenutzerInnen weitergeleitet und die BenutzerInnen für den verantwortungsvollen und vorsichtigen Umgang mit solchen E-Mails geschult und sensibilisiert werden,
- mit Hilfe von serverseitigen Tools in ein reines Textformat umgewandelt und danach mit einem entsprechenden Hinweis an die Benutzer weitergeleitet werden (dabei können allerdings Informationen verloren gehen),
- nicht direkt an die BenutzerInnen weitergeleitet werden, sondern an einen besonderen Arbeitsplatz, wo sie mit besonderen Sicherheitsvorkehrungen von den EmpfängerInnen eingesehen werden können (je nach E-Mail-Aufkommen kann dies allerdings einen nicht akzeptablen Aufwand mit sich bringen).

Grundsätzlich sollten alle BenutzerInnen für diese Problematik sensibilisiert sein.

12.4 Datensicherung

Unabdingbare Voraussetzung für jeden Business Continuity Plan ist die Planung und Durchführung einer ordnungsgemäßen Datensicherung.

12.4.1 Regelmäßige Datensicherung

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzeptes (vgl. 12.4.2 Entwicklung eines Datensicherungskonzeptes).

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist Folgendes festzulegen:

- Umfang der zu sichernden Daten:
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen. Z. B.: Sicherung der selbsterstellten Dateien und der individuellen Konfigurationsdateien.
- Zeitintervall:
  z. B. täglich, wöchentlich, monatlich
- Zeitpunkt:
  z. B. nachts, freitags abends
- Anzahl der aufzubewahrenden Generationen:
  bei täglicher Komplettsicherung werden z. B. die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabendsicherungen der letzten zwei Monate.
- Speichermedien (abhängig von der Datenmenge):
  z. B. Bänder, DVDs, Wechselplatten etc.
- Wiederaufbereitung der Datenträger (Löschung vor Wiederverwendung)
- Zuständigkeit für die Durchführung (Systemadministration, BenutzerIn)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung, gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollen zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. Werden zwischen zwei Komplettsicherungen mehrere inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.

Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist in der Regel die Aufbewahrung der Originaldatenträger und deren Sicherungskopien ausreichend. Sie braucht dann von der regelmäßigen Datensicherung nicht erfasst zu werden.

Alle BenutzerInnen sollten über die Regelungen zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der BenutzerInnen darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den BenutzerInnen oder automatisch dorthin überspielt werden.

12.4.2 Entwicklung eines Datensicherungskonzeptes

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist. Diese Lösung muss auch jederzeit aktualisierbar und erweiterbar sein. Weiters ist dafür Sorge zu tragen, dass alle betroffenen IT-Systeme im Datensicherungskonzept berücksichtigt werden und das Konzept stets den aktuellen Anforderungen entspricht.

Ein möglicher Aufbau eines Datensicherungskonzeptes ist in B Muster für Verträge, Verpflichtungserklärungen und Dokumentationen angeführt.

Einzelne Punkte eines Datensicherungskonzeptes werden in den nachfolgenden Maßnahmen näher ausgeführt.

Für die Gewährleistung einer funktionierenden Datensicherung müssen praktische Übungen zur Datenrestaurierbarkeit verpflichtend vorgesehen sein (siehe 17.2.2 Übungen zur Datenrekonstruktion).

12.4.3 Festlegung des Minimaldatensicherungskonzeptes

Für eine Organisation ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und damit auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde. Ein Beispiel soll dies erläutern.

Minimaldatensicherungskonzept (Beispiel):

- Software:
  Sämtliche Software, also sowohl Eigenentwicklungen als auch Standardsoftware, ist einmalig mittels einer Vollsicherung zu sichern.
- Systemdaten:
  Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.
- Anwendungsdaten:
  Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.
- Protokolldaten:
  Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

12.4.4 Datensicherung bei Einsatz kryptographischer Verfahren

Beim Einsatz kryptographischer Verfahren darf die Frage der Datensicherung nicht vernachlässigt werden. Neben der Frage, wie eine Datensicherung der verschlüsselten Daten sinnvollerweise erfolgen sollte, muss auch überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen. Daneben ist es auch zweckmäßig, die Konfigurationsdaten der eingesetzten Kryptoprodukte zu sichern.

Datensicherung der Schlüssel

Es muss sehr genau überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen, da jede Schlüsselkopie eine potenzielle Schwachstelle ist. Trotzdem kann es aus verschiedenen Gründen notwendig sein, kryptographische Schlüssel zu speichern.

Zu diesem Zweck bieten insbesondere kryptographische Produkte wie z.B. Hardware-Security-Module zertifizierte Backup-Funktionalitäten an. Ist eine solche Funktionalität vorhanden, sollte das Schlüsselmaterial nur durch eine solche zertifizierte Backup-Funktionalität gesichert werden, wodurch das Schlüsselmaterial nicht im Klartext exportierbar sein darf.

Es gibt unterschiedliche Methoden der Schlüsselspeicherung:

- die Speicherung zu Transportzwecken auf einem transportablen Datenträger, z. B. Chipkarte, USB-Stick (dient vor allem zur Schlüsselverteilung bzw. zum Schlüsselaustausch, siehe 10.1.7 Schlüsselmanagement),
- die Speicherung in IT-Komponenten, die dauerhaft auf kryptographische Schlüssel zugreifen müssen, also z. B. zur Kommunikationsverschlüsselung,
- die Schlüsselhinterlegung als Vorbeugung gegen Schlüsselverlust oder im Rahmen von Vertretungsregelungen.

Hierbei ist grundsätzlich zu beachten:

- Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht unbemerkt auslesen können. Beispielsweise könnten Schlüssel in spezieller Sicherheitshardware gespeichert werden, die die Schlüssel bei Angriffen automatisch löscht. Falls sie in Software gespeichert werden, sollten sie auf jeden Fall in verschlüsselter Form gespeichert werden. Hierbei ist zu bedenken, dass die meisten Standardanwendungen, bei denen Schlüssel oder Passwörter in der Anwendung gespeichert werden, dies i. Allg. mit leicht zu brechenden Verfahren tun. Als weitere Variante kann auch das Vier-Augen-Prinzip bei der Schlüsselspeicherung benutzt werden, also die Speicherung eines Schlüssels in Schlüsselhälften oder Schlüsselteilen.
- Von Kommunikationsschlüsseln und anderen kurzlebigen Schlüsseln sollten keine Kopien erstellt werden. Damit eine unautorisierte Nutzung ausgeschlossen ist, sollten auch von privaten Signaturschlüsseln i. Allg. keine Kopien existieren. Falls jedoch für die Schlüsselspeicherung eine reine Softwarelösung gewählt wurde, d. h. wenn keine Chipkarte o.ä. verwendet wird, ist das Risiko des Schlüsselverlustes (etwa durch Bitfehler oder Festplattendefekt) erhöht. In diesem Fall ist es unter Umständen weniger aufwendig, eine ausreichend gesicherte Möglichkeit der Schlüsselhinterlegung zu schaffen, als bei jedem Schlüsselverlust alle Kommunikationspartner zu informieren.
- Von langlebigen Schlüsseln, die z. B. zur Archivierung von Daten oder zur Generierung von Kommunikationsschlüsseln eingesetzt werden, sollten auf jeden Fall Sicherungskopien angefertigt werden.

Datensicherung der verschlüsselten Daten

> *Besondere Sorgfalt ist bei der Datensicherung von verschlüsselten Daten bzw. beim Einsatz von Verschlüsselung während der Datenspeicherung notwendig. Treten hierbei Fehler auf, sind nicht nur einige Datensätze, sondern meist alle Daten unbrauchbar.*

Die Langzeitspeicherung von verschlüsselten oder signierten Daten bringt viele zusätzliche Probleme mit sich. Hierbei muss nicht nur sichergestellt werden, dass die Datenträger regelmäßig aufgefrischt werden und jederzeit noch die technischen Komponenten zum Verarbeiten dieser zur Verfügung stehen, sondern auch, dass

die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen. Bei der langfristigen Archivierung von Daten kann es daher sinnvoller sein, diese unverschlüsselt zu speichern und dafür entsprechend sicher zu lagern, also z. B. in Tresoren.

Die verwendeten Kryptomodule sollten vorsichtshalber immer archiviert werden, da die Erfahrung zeigt, dass auch noch nach Jahren Daten auftauchen, die nicht im Archiv gelagert waren.

Datensicherung der Konfigurationsdaten der eingesetzten Produkte

> *Bei komplexeren Kryptoprodukten sollte nicht vergessen werden, deren Konfigurationsdaten zu sichern. Die gewählte Konfiguration sollte dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.*

12.4.5 Geeignete Aufbewahrung der Backup-Datenträger

Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.
- Ein ausreichend schneller Zugriff im Bedarfsfall muss gewährleistet sein.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner - auf jeden Fall in einem anderen Brandabschnitt, wenn möglich dislozierт - aufbewahrt werden.

Zu beachten sind auch die Anforderungen aus 8.3.2 Datenträgerverwaltung.

Je nach Anforderungen und geforderte Ausfallsicherheit (Katastrophenvorsorge – vgl. 17.1.1 Definition von Verfügbarkeitsklassen) kann es notwendig sein das Datenarchiv an einem gänzlich anderen Ort zu halten. Damit wird sichergestellt, dass der Datenbestand eines derartigen Notfallarchivs nicht aufgrund der gleichen Schadensursache zerstört wird, und dass im Falle der Unzugänglichkeit der Infrastruktur (beispielsweise aufgrund von Verschüttungen, o.ä.) der Datensicherungsbestand zur Verfügung steht.

12.4.6 Sicherungskopie der eingesetzten Software

Von den Originaldatenträgern von Standardsoftware bzw. von der Originalsoftware bei Eigenentwicklungen ist - sofern möglich - eine Sicherungskopie zu erstellen, von der bei Bedarf die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren. Es ist darauf zu achten, dass der physikalische Schreibschutz des Datenträgers ein versehentliches Löschen oder Überschreiben der Daten verhindert.

Ein unerlaubter Zugriff, z. B. zur Erstellung einer Raubkopie, muss ausgeschlossen sein.

12.4.7 Beschaffung eines geeigneten Datensicherungssystems

Ein Großteil der Fehler, die beim Erstellen oder Restaurieren einer Datensicherung auftreten, sind Fehlbedienungen. Daher sollte bei der Beschaffung eines Datensicherungssystems nicht allein auf dessen Leistungsfähigkeit geachtet werden, sondern auch auf seine Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Bei der Auswahl von Sicherungssoftware sollte darauf geachtet werden, dass sie die folgenden Anforderungen erfüllt:

- Die Datensicherungssoftware sollte ein falsches Medium ebenso wie ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, ausgewählte BenutzerInnen automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort oder, je nach Vertraulichkeitsanforderungen, durch Verschlüsselung unterstützen. Weiters sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.

- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die zu sichernden Daten sollten auch auf Festplatten und Netzlaufwerken abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch ein Passwort geschützt werden kann, sollte diese Option genutzt werden.

12.4.8 Datensicherung bei mobiler Nutzung eines IT-Systems

IT-Systeme im mobilen Einsatz (z. B. Notebooks, Tablets, Smartphones) sind in aller Regel nicht permanent in ein Netz eingebunden, aber meist besteht eine aufrechte Internetverbindung. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

Datensicherung auf externen Datenträgern

Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk und genügend Datenträger mitgeführt werden müssen und dass für die BenutzerInnen zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht.

Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, so dass die BenutzerInnen nicht mehrere Datenträger pro Sicherungsvorgang in das Laufwerk einlegen müssen. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhandenkommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhandenkommen.

Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Organisation eingebracht werden.

Datensicherung über temporäre Netzverbindungen

Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass die BenutzerInnen keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen müssen. Weiters lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.

Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn die BenutzerInnen gleichzeitig auf entfernte Ressourcen zugreifen müssen. Bei manchen Zugangstechnologien (z. B. Mobiltelefon bzw. Smartphone, Tablet) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen, hierdurch erhöht sich jedoch u.U. der Aufwand für die Wiederherstellung einer Datensicherung.

12.4.9 Verpflichtung der MitarbeiterInnen zur Datensicherung

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahme darstellt, sollten die betroffenen MitarbeiterInnen - vorzugsweise in schriftlicher Form - zur Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Motivation zur Datensicherung und Kontrolle auf Einhaltung ist empfehlenswert.

12.5 Protokollierung und Monitoring

12.5.1 Erstellung von Protokolldateien

Art und Umfang von Protokollierungen hängen von den speziellen Anforderungen des IT-Systems und der darauf befindlichen Applikationen und Daten ab und sind im Einzelfall sorgfältig festzulegen. Die im Folgenden angeführten Anforderungen an die Protokollierung stellen Mindestanforderungen dar, wie sie für die meisten Systeme Gültigkeit haben.

Demnach sind bei der Administration von IT-Systemen die folgenden Aktivitäten vollständig zu protokollieren:

- Systemgenerierung und Modifikation von Systemparametern:
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.
- Einrichten von BenutzerInnen:
  Es ist vollständig zu protokollieren, wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen. Diese Protokolle sind Grundlage praktisch jeder Revisionsmaßnahme.
- Erstellung von Rechteprofilen:
  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat.
- Einspielen und Änderung von Anwendungssoftware:

Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

- Änderungen an der Dateiorganisation:
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der „Standard-Dateiverwaltungssysteme“ ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (vgl. z. B. Datenbankmanagement).
- Durchführung von Datensicherungsmaßnahmen:
  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in „Ausnahmesituationen“ durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.
- Sonstiger Aufruf von Administrations-Tools:
  Die Benutzung aller Administrations-Tools ist zu dokumentieren, um feststellen zu können, ob Unbefugte sich Systemadministratorrechte erschlichen haben.
- Versuche unbefugten Einloggens und Überschreitung von Befugnissen:
  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller „auffälligen Abnormitäten“ beim Einloggen und der Benutzung von Hard- und Softwarekomponenten eine zentrale Bedeutung zu. BenutzerInnen in diesem Sinne sind auch SystemadministratorInnen.

Um eine ordnungsgemäße Auswertung der Protokolldaten zu ermöglichen ist zu beachten:

- Die Speicherung der Protokolldaten hat in einer nicht manipulierbaren Form zu erfolgen (die Daten dürfen nicht gezielt verändert, unbefugt gelöscht oder zerstört werden können).
- Nicht-personenbezogene IDs sind zu vermeiden, da sie eine personenbezogene Auswertung unmöglich machen.
- Das Überschreiben eines bestimmten protokollierten Ereignisses durch ein gezieltes Auffüllen des Speichers der Protokolldaten mit „unverdächtigen“ Daten muss zuverlässig verhindert werden.
- Die Entscheidung, welche Daten zu protokollieren sind, haben Datenschutzbeauftragte/CISOs oder Applikationsverantwortliche in Übereinstimmung mit gesetzlichen Vorgaben (etwa Datenschutzgesetz und DSGVO) und der organisationsweiten IT-Sicherheitspolitik zu treffen. Dabei ist es wichtig, sich auf die tatsächlich relevanten Informationen zu beschränken, da ein zu großer Umfang an Daten die Auswertung der Daten erschweren oder sogar unmöglich machen kann.

12.5.2 Datenschutzrechtliche Aspekte bei der Erstellung von Protokolldateien

Laut Artikel 32 DSGVO (Sicherheit der Verarbeitung) sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Daher sind unter anderem verschiedene Kontrollen zu implementieren, um beispielsweise die Verarbeitung, das Lesen und die Änderung personenbezogener Daten festzustellen und nachvollziehen zu können, d.h. jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann. Im sicherheitspolizeilichen Bereich ist diesbezüglich insbesondere § 50 DSG zu beachten.

Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung einschließlich der Eigenüberwachung, der Gewährleistung von Integrität und Sicherheit der personenbezogenen Daten sowie in gerichtlichen Strafverfahren verwendet werden.

Aufbewahrungsfristen/Löschfristen

Konkrete Aufbewahrungsfristen für Protokoll- und Dokumentationsdaten sind in der DSGVO bzw. im aktuellen Datenschutzgesetz nicht mehr festgelegt. Sie müssen vielmehr für einen je nach Art und Inhalt der protokollierten Ereignisse bzw. dem Ergebnis der Risikobewertung entsprechend angemessenen Zeitraum aufbewahrt werden. Protokolldaten sind – in personenbezogener Form – zu löschen, sobald die Zwecke für die sie erhoben wurden, erreicht wurden und auch keine sonstigen gesetzlichen Aufbewahrungsfristen bestehen. Beispielsweise können Protokolldaten mit Personenbezug, anonymisiert werden, sofern nur noch Metadaten des protokollierten Ereignisses relevant sind.

Diese Pflichten gelten nur für den Gebrauch von personenbezogenen Daten. Protokollierungen von Daten, die nicht personenbezogenen sind, wie z. B. die Installation eines Servers, Aufzeichnungen über den Datendurchsatz eines Systems etc., sind nicht betroffen.

12.5.3 Kontrolle von Protokolldateien

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Ist es personell oder technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu implementieren, kann ihre Auswertung auch durch die AdministratorInnen erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten der AdministratorInnen nur schwer möglich ist. Den Datenschutzbeauftragten/CISOs ist jedenfalls eine derartige Auswertung vorzulegen.

Die regelmäßige Kontrolle dient darüber hinaus auch dem Zweck, durch die anschließende Löschung der Protokolldaten ein übermäßiges Anwachsen der Protokolldateien zu verhindern.

Je nach Art der Protokolldaten kann es sinnvoll sein, diese auf externen Datenträgern zu archivieren.

Da Protokolldateien in vielen Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur für Zwecke, die mit ihrem Ermittlungszweck vereinbar sind, verwendet werden dürfen (vgl. Artikel 5 DSGVO). Diese Einschränkung kann gelöst werden, indem die personenbezogenen Daten entfernt oder anonymisiert (nicht jedoch pseudonymisiert) werden.

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?
- Gibt es auffallend lange Verbindungszeiten in öffentliche Netze hinein?
- Wurde in einzelnen Netzsegmenten oder im gesamten Netz eine auffällig hohe Netzlast oder eine Unterbrechung des Netzbetriebes festgestellt (Hinweis auf Versuche, die Dienste des Netzes zu verhindern bzw. zu beeinträchtigen oder auf eine ungeeignete Konzeption bzw. Konfiguration des Netzes)?

Bei der Auswertung der Protokolldateien sollte besonderes Augenmerk auf alle Zugriffe gelegt werden, die unter Administratorkennungen durchgeführt wurden.

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfacher fehlerhafter Anmeldeversuch) hervorheben.

Weiters ist zu beachten:

- Die Verantwortung für die Auswertung der Protokolldaten ist genau festzulegen.
- In besonders sicherheitskritischen Fällen sollte das Vier-Augen-Prinzip zur Anwendung kommen.
- Die Meldewege im Fall von Auffälligkeiten sind festzulegen.
- Es ist sicherzustellen, dass die Aktivitäten von AdministratorInnen ausreichend kontrolliert werden können. Diese Sicherstellung kann durch technische oder organisatorische Maßnahmen erfolgen.

12.5.4 Rechtliche Aspekte bei der Erstellung und Auswertung von Protokolldateien zur E-Mail- und Internetnutzung

Bezug: Österreich

Die Überwachung des Fernmeldeverkehrs (Telefon, E-Mail etc.) durch den Arbeitgeber ist ein Problem, für das es derzeit noch keine klare Lösung gibt. Private Kommunikation genießt prinzipiell den Schutz des Fernmeldegeheimnisses und des Grundrechtes auf Datenschutz. Es muss aber auch gesagt werden, dass kein Recht der ArbeitnehmerInnen besteht, die vom Arbeitgeber zur Verfügung gestellten Ressourcen privat zu nutzen. Eine geringfügige private oder halbprivate Nutzung im Rahmen des normalen menschlichen Sozialverhaltens sollte zugelassen bzw. ignoriert werden. Ein totales Verbot privater Nutzung sollte nur in Extremfällen ausgesprochen werden (z. B. bei Behörden mit sehr hohen Ansprüchen an Sicherheit und Geheimhaltung).

Ein Arbeitgeber, der die private Nutzung von Internetdiensten einschränken will, sollte sich über die Gründe im Klaren sein.

- Der Hauptgrund werden die Kosten sein, die durch private Kommunikation verursacht werden, und zwar die direkten Kosten (Bandbreite, Speicherplatz) als auch der Verlust an Produktivität.
- Ein weiterer Grund für die Beschränkung privater E-Mail-Kommunikation kann im Schutz vor Viren, Trojanern und anderer schädlicher Software liegen.

Eine Vereinbarung zu diesem Thema ist wünschenswert. Gemäß § 9 Abs. 2 lit. f Bundes-Personalvertretungsgesetz (PVG) ist bei der Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Bediensteten, die über die Ermittlung von allgemeinen Angaben zur Person oder über die Ermittlung von fachlichen Voraussetzungen hinausgehen, mit dem Dienststellenausschuss das Einvernehmen herzustellen.

Gemäß § 79e Beamten-Dienstrechtsgesetz 1979 (BDG 1979), § 29n Vertragsbedienstetengesetz 1948 (VBG) und § 76g Richter- und Staatsanwaltschaftsdienstgesetz (RStDG) ist die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, unzulässig, wobei die Frage, welche Maßnahmen die Menschenwürde berühren, interpretiert werden muss. Die Erläuterungen zu den Bestimmungen (1574 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP) verweisen auf die Judikatur zu § 96 Arbeitsverfassungsgesetz (ArbVG).

Die Rechte des Arbeitgebers auf Schutz seiner IKT-Einrichtungen (insbesondere Gebrauch von Virenscannern) bleiben unberührt.

Die Gefahr von Virenbefall, Trojanern und anderer schädlicher Software lässt sich mit Hilfe geeigneter technischer Mittel stark reduzieren, insbesondere Virenscanner, Begrenzung des Rechts zur Installation ausführbarer Programme, Gebrauch von stabiler Systemsoftware, Einrichtung von kontrollierten Umgebungen zur Ausführung fragwürdiger Programme etc.

Behörden, die im Rahmen des E-Governments tätig sind, werden rasch auf ein ernstes Problem stoßen: Den Nachweis von Zustellungen per E-Mail. Solange keine zuverlässigen Verfahren für E-Mail-Zustellbestätigungen existieren, begründet der protokollierte Postausgang zumindest den Anschein einer korrekten Versendung durch die Behörde. Der protokollierte Posteingang wiederum macht es unseriösen Elementen schwer, falsche Behauptungen aufzustellen („Ich habe alles rechtzeitig mit E-Mail beantragt …“). Eine Aufzeichnung und Speicherung aller E-Mails (oder auch nur von Teilen, wie z. B. der Betreffzeile, Datum, Uhrzeit, Absender- und Empfängeradresse) kann die oben genannten Probleme verschärfen, aber auch die BeamtInnen bei ihrer Tätigkeit unterstützen.

Falls ein dienstliches Interesse an der Verwendung von E-Mail für nicht unmittelbar dienstliche Zwecke besteht (z. B. Zusendung von Informationen durch die Personalvertretung), sollten derartige E-Mails von jeglicher Kontrolle ausgenommen werden. Weiters dürfen E-Mails an die Personalvertretung durch den Arbeitgeber inhaltlich nicht kontrolliert werden.

§ 26 Bundes-Personalvertretungsgesetz (PVG) statuiert eine Geheimhaltungspflicht der Mitglieder der Personalvertretung über alle ihnen von einzelnen Bediensteten gemachten Mitteilungen, die der Sache nach oder auf Wunsch der Bediensteten vertraulich zu behandeln sind. Eine Erfassung von Telefondaten, mit der

sich nachvollziehen lässt, mit wem ein Personalvertreter telefonisch in Kontakt war, widerspricht daher dem Datenschutzgesetz (Entscheidung der Datenschutzkommission vom 06.10.1998, Zahl 120.599/8-DSK/98). Diese Entscheidung lässt sich auch auf E-Mail übertragen.

12.5.5 Audit und Protokollierung der Aktivitäten im Netz

Eine angemessene Durchführung von Protokollierung, Audit und Revision ist ein wesentlicher Faktor der Netzsicherheit.

Protokollierung

Eine Protokollierung innerhalb eines Netzmanagementsystems oder an bestimmten aktiven Netzkomponenten erlaubt es, gewisse (i. Allg. zu definierende) Zustände für eine spätere Auswertung abzuspeichern. Typische Fälle, die protokolliert werden können, sind z. B. die übertragenen fehlerhaften Pakete an einer Netzkomponente, ein unautorisierter Zugriff auf eine Netzkomponente oder die Performance eines Netzes zu bestimmten Zeiten. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Bei der Protokollierung fallen zumeist sehr viele Einträge an, so dass diese oft nur mit Hilfe eines Werkzeuges sinnvoll ausgewertet werden können.

Audit

Unter einem Audit wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Dies kann online oder offline erfolgen. Bei einem Online-Audit werden die Ereignisse mit Hilfe eines Tools (z. B. einem Netzmanagementsystem) in Echtzeit betrachtet und ausgewertet. Bei einem Offline-Audit werden die Daten protokolliert oder aus einer bestehenden Protokolldatei extrahiert.

Beim Audit liegt die Fokussierung auf der Überwachung von sicherheitskritischen Ereignissen. Zusätzlich werden beim Audit häufig auch Daten über Nutzungszeiträume und anfallende Kosten erhoben.

Dabei sind für ein Audit insbesondere folgende Vorkommnisse von Interesse:

- Daten über die Betriebsdauer von IT-Systemen (wann wurde welches IT-System ein- bzw. wieder ausgeschaltet?),
- Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?),
- sicherheitskritische Zugriffe auf Netzkomponenten und Netzmanagementkomponenten mit oder ohne Erfolg,

- Verteilung der Netzlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance des Netzes.

Weiterhin sollten folgende Vorkommnisse protokolliert werden:

- Hardwarefehlfunktionen, die zu einem Ausfall eines IT-Systems führen können,
- unzulässige Änderungen der IP-Adresse eines IT-Systems (in einem TCP/IP-Umfeld).

Ein Audit kann sowohl online als auch offline betrieben werden. Bei einem Online-Audit werden entsprechend kategorisierte Ereignisse direkt dem Auditor mitgeteilt, der ggf. sofort Maßnahmen einleiten kann. Dafür müssen Ereignisse in geeignete Kategorien eingeteilt werden, damit die zuständigen AdministratorInnen oder AuditorInnen auf wichtige Ereignisse sofort reagieren können und nicht unter einer Flut von Informationen den Überblick verlieren. Dabei ist auch zu überlegen, ob eine Rollentrennung erforderlich ist.

Bei einem Offline-Audit werden die Daten aus den Protokolldateien oder speziellen Auditdateien mit Hilfe eines Werkzeuges für Auditzwecke aufbereitet und durch die AuditorInnen überprüft. Im letzten Fall können Maßnahmen zur Einhaltung oder Wiederherstellung der Sicherheit nur zeitverzögert eingeleitet werden. I. Allg. wird eine Mischform aus Online- und Offline-Audit empfohlen. Dabei werden für das Online-Audit die sicherheitskritischen Ereignisse gefiltert und den AuditorInnen sofort zur Kenntnis gebracht. Zusätzlich werden weniger kritische Ereignisse offline ausgewertet.

Revision

Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von unabhängigen MitarbeiterInnen (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der AdministratorInnen zu kontrollieren. Die mit einem Netzmanagementsystem möglichen Protokollierungs- und Audit-Funktionen sind in einem sinnvollen Umfang zu aktivieren. Neben Performance-Messungen zur Überwachung der Netzlast sind dabei insbesondere die Ereignisse (Events) auszuwerten, die von einem Netzmanagementsystem generiert werden, oder spezifische Datensammler einzusetzen, mit denen sicherheitskritische Ereignisse überwacht und ausgewertet werden können.

Auf keinen Fall dürfen Benutzerpasswörter im Rahmen eines Audits oder einer Protokollierung gesammelt werden. Dadurch wird ein hohes Sicherheitsrisiko erzeugt, falls es zu einem unberechtigten Zugriff auf diese Informationen kommt. Ob falsch eingegebene Passwörter, die sich von den gültigen Passwörtern meist nur um ein Zeichen bzw. um eine Vertauschung zweier Zeichen unterscheiden, protokolliert werden, ist im Einzelfall zu entscheiden.

Es muss weiters festgelegt werden, wer die Protokolle und Audit-Daten auswertet. Hierbei muss eine angemessene Trennung zwischen EreignisverursacherInnen und -auswerterInnen (z. B. AdministratorInnen und AuditorInnen) vorgenommen werden. Weiterhin ist darauf zu achten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden.

Die Protokoll- oder Auditdateien müssen regelmäßig ausgewertet werden. Sie können sehr schnell sehr umfangreich werden. Um die Protokoll- oder Auditdateien auf ein auswertbares Maß zu beschränken, sollten die Auswertungsintervalle daher angemessen, aber dennoch so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist.

12.5.6 Intrusion Detection Systeme

Aufgabe von Intrusion Detection Systemen ist die Überwachung bzw. Analyse des Datenverkehrs bzw. der Aktivitäten auf IT-Systemen, mit dem Ziel, Eindringversuche zu erkennen, weiterzumelden und gegebenenfalls Gegenmaßnahmen einzuleiten.

Dies umfasst folgende Teilaufgaben:

- Erfassung von Ereignissen:
  Sammlung der wesentlichen Ereignisdaten aus Netzpaketen oder Protokolldateien
- Analyse der erfassten Ereignisse:
  Untersuchung der gespeicherten Aktivitäten auf Auffälligkeiten (z. B. anormales Verhalten von BenutzerInnen („Anomalie Intrusion Detection Systeme“) oder bekannte Befehlsmuster („Misuse Intrusion Detection Systeme“))
- Speicherung der analysierten Daten
- Einleitung von Gegenmaßnahmen:
  Generierung von Warnmeldungen und Setzen von Gegenmaßnahmen (dann spricht man von „Intrusion Prevention Systemen“)

Im Unterschied zu Firewalls, die die Anbindung eines Netzwerkes an ein Fremdnetz (etwa Internet) absichern, unterstützen Intrusion Detection Systeme die Erkennung unberechtigter Zugriffsversuche sowohl externer als auch interner BenutzerInnen innerhalb eines lokalen Netzes.

Intrusion Detection Systeme können andere Sicherheitsmaßnahmen, wie Authentisierung, Zugriffsschutzsysteme und Firewalls nicht ersetzen, sie können jedoch zu einer weiteren Erhöhung der Sicherheit, insbesondere in sensiblen Bereichen, beitragen.

12.5.7 Zeitsynchronisation

In vielen Situationen ist es bei vernetzten Systemen wichtig, dass alle bei einem Vorgang betroffenen Rechner eine korrekte Systemzeit besitzen. Insbesondere bei der Auswertung von Protokollierungsinformationen ist dies von zentraler Bedeutung, beispielsweise um Fehlermeldungen, die auf einen Angriff über das Netz hindeuten, richtig korrelieren zu können, oder wenn bei Anwendungen, die über mehrere Rechner verteilt sind, Synchronisationsprobleme auftreten. Auch verteilte Dateisysteme und zentrale Authentisierungsdienste sind auf Zeitsynchronizität angewiesen.

Für die korrekte Einstellung der Systemzeit bieten die meisten Betriebssysteme die Möglichkeit, über das Protokoll NTP (Network Time Protocol Version 4 [RFC 5905]) auf einen externen Zeitserver zuzugreifen. Windows-Rechner in einer Active Directory Infrastruktur gleichen zudem die Systemzeit mit dem Domänencontroller ab.

Im Internet existiert eine verteilte Infrastruktur von öffentlichen NTP-Zeitservern.

Da NTP ein Klartextprotokoll ohne kryptographische Sicherungen ist, sollte es nur innerhalb des eigenen Netzes eingesetzt werden. Falls die Zeitserver-Infrastruktur im Internet genutzt werden soll, so sollte dafür ein eigener Rechner vorgesehen werden, der als einziger die NTP-Informationen von den ausgewählten Zeitservern bezieht. Die Rechner im lokalen Netz synchronisieren ihre Systemuhr dann mit dem lokalen NTP-Proxy. An der Firewall sollte NTP in diesem Fall nur für den NTP-Proxy-Server freigeschaltet werden. Insbesondere in Netzen mit hohem Schutzbedarf sollten keinesfalls alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.

Alternativ kann ein Rechner im internen Netz mit einem Funkuhr-Modul ausgestattet als lokaler Zeitserver eingesetzt werden. Im Zweifelsfall sollte dieser Lösung der Vorzug gegeben werden.

Falls für die Zeitsynchronisation auf externe Quellen (Funkuhren, öffentliche NTP-Zeitserver etc.) zurückgegriffen wird, muss sichergestellt werden, dass die empfangenen Zeit-Informationen nicht ungeprüft übernommen werden. Die Software des lokalen Zeit-Servers beziehungsweise NTP-Proxys muss eine Plausibilitätsprüfung vornehmen, bevor sie die empfangenen Zeit-Informationen übernimmt und an die anderen Rechner im Netz weitergibt. Ein Beispiel für eine solche Plausibilitätsprüfung ist, dass sprunghafte Änderungen, die eine vorher festgelegte maximale Zeitdifferenz überschreiten, nicht übernommen werden.

13 Sicherheitsmanagement in der Kommunikation

13.1 Netzsicherheit

Zur Unterstützung der System-/Netzwerkadministration ist der Einsatz von entsprechenden Tools (z. B. CAD-Programmen, speziellen Tools für Netzpläne, Kabelmanagementtools im Zusammenhang mit Systemmanagementtools o.ä.) empfehlenswert. Eine konsequente Aktualisierung aller Informationen bei Umbauten oder Erweiterungen ist ebenso zu gewährleisten wie eine eindeutige und nachvollziehbare Dokumentation (vgl. auch 11.4.1 Lagepläne der Versorgungsleitungen).

Gerade im Zusammenhang mit dem Absichern von Netzwerken gibt es eine Reihe weiterführender Literatur. Exemplarisch sei an dieser Stelle „The 60 Minute Network Security Guide“ der NSA [NSA-SD7] genannt.

13.1.1 Sicherstellung einer konsistenten Systemverwaltung

In vielen komplexen IT-Systemen gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Missbrauch besonders hoch.

Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist. Andere Arbeiten sollen auch die AdministratorInnen nicht unter der Administratorkennung erledigen. Insbesondere dürfen keine Programme anderer BenutzerInnen unter der Administratorkennung aufgerufen werden. Ferner sollte die routinemäßige Systemverwaltung (z. B. Backup, Einrichten neuer BenutzerInnen) nur menügesteuert durchgeführt werden können.

Für alle AdministratorInnen sind zusätzliche Benutzerkennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die AdministratorInnen zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, sollen die AdministratorInnen ausschließlich diese zusätzlichen Benutzerkennungen verwenden.

Falls das Betriebssystem erlaubt, sollten die AdministratorInnen grundsätzlich nicht als Superuser, sondern unter ihrer persönlichen Benutzerkennung einsteigen und erst dann in die Superuser-Rolle wechseln.

Bekannte Kennungen, wie etwa root, guest oder administrator, sind zu löschen, stillzulegen oder nach Bedarf zu modifizieren. Bekannte Passwörter (Firmenkennungen und Firmen-Passwörter) sind zu löschen bzw. zu ändern, insbesondere bei Netzwerkkomponenten (Router, Switches, …).

Alle durchgeführten Änderungen sollten dokumentiert werden, um diese nachvollziehbar zu machen und die Aufgabenteilung zu erleichtern.

13.1.2 Ist-Aufnahme der aktuellen Netzsituation

Die Bestandsaufnahme der aktuellen Netzsituation ist Voraussetzung für

- eine gezielte Sicherheitsanalyse des bestehenden Netzes sowie für
- die Erweiterung eines bestehenden Netzes.

Hierzu ist eine Ist-Aufnahme mit einhergehender Dokumentation der folgenden Aspekte, die z.T. aufeinander aufbauen, notwendig:

- Netztopographie,
- Netztopologie,
- verwendete Netzprotokolle,
- Kommunikationsübergänge im LAN und zum WAN sowie
- Netzperformance und Verkehrsfluss.

Unter der Topographie eines Netzes wird die rein physikalische Struktur eines Netzes in Form der Kabelführung verstanden. Im Gegensatz dazu handelt es sich bei der Netztopologie um die logische Struktur eines Netzes. Die Topographie und Topologie eines Netzes sind nicht notwendig identisch.

13.1.3 Analyse der aktuellen Netzsituation

Diese Maßnahme baut auf den Ergebnissen der Ist-Aufnahme nach 13.1.2 Ist-Aufnahme der aktuellen Netzsituation auf und erfordert spezielle Kenntnisse im Bereich der Netztopologie, der Netztopographie und von netzspezifischen Schwachstellen. Darüber hinaus ist Erfahrung bei der Beurteilung der eingesetzten individuellen IT-Anwendungen hinsichtlich Vertraulichkeit, Integrität bzw. Verfügbarkeit notwendig.

Eine Analyse der aktuellen Netzsituation besteht im Wesentlichen aus einer Strukturanalyse, einer Schutzbedarfsfeststellung und einer Schwachstellenanalyse.

Strukturanalyse

Diese besteht aus einer Analyse der nach 13.1.2 Ist-Aufnahme der aktuellen Netzsituation angelegten Dokumentationen. Die Strukturanalyse muss von einem Analyseteam durchgeführt werden, das in der Lage ist, alle möglichen Kommunikationsbeziehungen nachzuvollziehen oder auch herleiten zu können.

Als Ergebnis muss das Analyseteam die Funktionsweise des Netzes verstanden haben und über die prinzipiellen Kommunikationsmöglichkeiten informiert sein. Häufig lassen sich bei der Strukturanalyse bereits konzeptionelle Schwächen des Netzes identifizieren.

Detaillierte Schutzbedarfsfeststellung

Bei besonders schutzwürdigen Applikationen sind in einer detaillierten Schutzbedarfsfeststellung zusätzlich die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität in einzelnen Netzbereichen bzw. Segmenten zu berücksichtigen.

Hierzu ist es notwendig festzustellen, welche Anforderungen aufgrund der verschiedenen IT-Verfahren bestehen und wie diese auf die gegebene Netzsegmentierung Einfluss nehmen. Als Ergebnis muss erkenntlich sein, in welchen Netzsegmenten besondere Sicherheitsanforderungen bestehen.

Analyse von Schwachstellen im Netz

Basierend auf den bisher vorliegenden Ergebnissen erfolgt eine Analyse der Schwachpunkte des Netzes.

Hierzu gehört insbesondere bei entsprechenden Verfügbarkeitsanforderungen die Identifizierung von nicht redundant ausgelegten Netzkomponenten (Single-Point-of-Failures). Weiters müssen die Bereiche benannt werden, in denen die Anforderungen an Verfügbarkeit, Vertraulichkeit oder Integrität nicht eingehalten werden können bzw. besonderer Aufmerksamkeit bedürfen. Zudem ist festzustellen, ob die gewählte Segmentierung hinsichtlich Bandbreite und Performance geeignet ist.

Es ist zu beachten, dass diese Maßnahme insbesondere in der Designphase für ein neues Netz oder einen neuen Netzteil sinnvoll ist, Änderungen in bestehenden Netzen können aus wirtschaftlichen Aspekten oft sehr schwierig sein.

13.1.4 Entwicklung eines Netzkonzeptes

Um den Anforderungen bezüglich Verfügbarkeit (auch Bandbreite und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung eines Netzes sorgfältig geplant werden. Hierzu dient die Erstellung eines Netzkonzeptes.

Die Entwicklung eines Netzkonzeptes unterteilt sich in einen analytischen und einen konzeptionellen Teil:

Analyse

Zunächst ist zu unterscheiden, ob ein bestehendes Netz zu erweitern bzw. zu verändern ist oder ob das Netz vollständig neu aufgebaut werden soll.

Im ersten Fall sind vorab die Maßnahmen 13.1.2 Ist-Aufnahme der aktuellen Netzsituation und 13.1.3 Analyse der aktuellen Netzsituation zu bearbeiten. Im zweiten Fall entfallen diese Maßnahmen. Stattdessen sind die Anforderungen an die Netzkommunikation zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Zur Ermittlung der Kommunikationsanforderungen ist der zukünftig zu erwartende Daten- und Verkehrsfluss zwischen logischen oder organisatorischen Einheiten festzustellen, da die zu erwartende Last die Segmentierung des zukünftigen Netzes beeinflussen muss. Die notwendigen logischen bzw. physikalischen Kommunikationsbeziehungen (dienste-, anwender-, gruppenbezogen) sind ebenfalls zu eruieren und die Kommunikationsübergänge zur LAN/LAN-Kopplung oder über ein WAN zu ermitteln.

Die Schutzbedarfsanforderungen des Netzes werden aus denen der geplanten oder bereits bestehenden IT-Verfahren abgeleitet. Daraus werden physikalische und logische Segmentstrukturen gefolgert, so dass diesen Anforderungen (z. B. hinsichtlich Vertraulichkeit) durch eine Realisierung des Netzes Rechnung getragen werden kann. Zum Beispiel bestimmt der Schutzbedarf einer IT-Anwendung die zukünftige Segmentierung des Netzes.

Schließlich muss versucht werden, die abgeleiteten Kommunikationsbeziehungen mit den Schutzbedarfsanforderungen zu harmonisieren. Unter Umständen sind hierzu Kommunikationsbeziehungen einzuschränken, um dem festgestellten Schutzbedarf gerecht zu werden.

Abschließend sind die verfügbaren Ressourcen zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen.

Die Ergebnisse sind entsprechend zu dokumentieren.

Konzeption

Im nächsten Schritt sind die Netzstruktur und die zu beachtenden Randbedingungen zu entwickeln. Dabei sind neben den oben genannten Gesichtspunkten auch die künftig zu erwartenden Anforderungen (z. B. hinsichtlich Bandbreite) sowie die örtlichen Gegebenheiten zu berücksichtigen.

Die Erstellung eines Netzkonzeptes erfolgt analog 13.1.2 Ist-Aufnahme der aktuellen Netzsituation und besteht danach prinzipiell aus den folgenden Schritten, wobei diese Schritte nicht in jedem Fall streng aufeinander folgend ausgeführt werden können. In einigen Teilen beeinflussen sich die Ergebnisse der Schritte gegenseitig, so dass eine regelmäßige Überprüfung und Konsolidierung der Teilergebnisse vorgenommen werden muss.

1. Konzeption der Netztopographie und der Netztopologie, der physikalischen und logischen Segmentierung
2. Konzeption der verwendeten Netzprotokolle
3. Konzeption von Kommunikationsübergängen im LAN und WAN

13.1.5 Entwicklung eines Netzmanagementkonzeptes

Netzmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven Einsatzes eines Netzes. Hierzu gehört beispielsweise die Überwachung der Netzkomponenten auf ihre korrekte Funktion, das Monitoring der Netzperformance und die zentrale Konfiguration der Netzkomponenten.

Netzmanagement ist in erster Linie eine organisatorische Problemstellung, deren Lösung mit technischen Mitteln - einem Netzmanagementsystem - lediglich unterstützt werden kann. Abzugrenzen vom Netzmanagement ist das Systemmanagement, welches sich in erster Linie mit dem Management verteilter Systeme befasst. Hierzu gehören beispielsweise eine zentrale Verwaltung der BenutzerInnen, Softwareverteilung, Management der Anwendungen usw. In einigen Bereichen, wie z. B. dem Konfigurationsmanagement (dem Überwachen und Konsolidieren von Konfigurationen eines Systems oder einer Netzkomponente) sind Netz- und Systemmanagement nicht klar zu trennen. In der ISO/IEC-Norm 7498-4 bzw. als X.700 der ITU-T ([ITU-T]) ist ein Netz- und Systemmanagement-Framework definiert.

Vor der Beschaffung und dem Betrieb eines solchen Netzmanagementsystems ist im ersten Schritt ein Konzept zu erstellen, in dem alle Sicherheitsanforderungen an das Netzmanagement formuliert und angemessene Maßnahmen für den Fehler- oder Alarmfall vorgeschlagen werden. Dabei sind insbesondere die folgenden Bestandteile eines Netzmanagementkonzeptes bei der Erstellung zu berücksichtigen und in einem Gesamtzusammenhang darzustellen:

- Performancemessungen zur Netzanalyse (siehe 13.1.3 Analyse der aktuellen Netzsituation),
- Reaktionen auf Fehlermeldungen der überwachten Netzkomponenten,
- Fernwartung/Remote-Control, insbesondere der aktiven Netzkomponenten,
- Generierung von Trouble-Tickets und Eskalation bei Netzproblemen,
- Protokollierung und Audit (online oder offline),
- Einbindung eventuell vorhandener proprietärer Systeme bzw. von Systemen mit unterschiedlichen Managementprotokollen (z. B. im Telekommunikationsbereich),
- Konfigurationsmanagement aller im Einsatz befindlichen IT-Systeme,
- verteilter Zugriff auf die Netzmanagementfunktionalitäten. (Für die Administration oder für das Audit kann ein Remotezugriff auf die Netzmanagementfunktionalitäten notwendig sein. Hier ist insbesondere eine sorgfältige Definition und Vergabe der Zugriffsrechte notwendig.)

13.1.6 Sicherer Betrieb eines Netzmanagementsystems

Für den sicheren Betrieb eines Netzmanagementtools oder eines komplexen Netzmanagementsystems, welches beispielsweise aus mehreren verschiedenen Netzmanagementtools zusammengesetzt sein kann, ist die sichere Konfiguration aller beteiligten Komponenten zu überprüfen und sicherzustellen. Hierzu gehören die Betriebssysteme, auf denen das oder die Netzmanagementsysteme betrieben werden, die zumeist notwendigen externen Datenbanken für ein Netzmanagementsystem, das verwendete Protokoll und die aktiven Netzkomponenten selbst. Vor dem Betrieb eines Netzmanagementsystems muss die Ermittlung der Anforderungen an den Betrieb und die Erstellung eines Netzmanagementkonzeptes stehen (siehe 13.1.5 Entwicklung eines Netzmanagementkonzeptes).

Für den sicheren Betrieb eines Netzmanagementsystems sind folgende Daten relevant:

- Konfigurationsdaten des Netzmanagementsystems, die sich in entsprechend geschützten Verzeichnissen befinden müssen.
- Konfigurationsdaten der Netzkomponenten (Metakonfigurationsdateien), die sich ebenfalls in entsprechend geschützten Verzeichnissen befinden müssen.
- Passwortdateien für das Netzmanagementsystem. Hierbei ist beispielsweise auf die Güte des Passwortes und die Möglichkeit einer verschlüsselten Speicherung des Passwortes zu achten.
- Eine Administration der aktiven Netzkomponenten über das Netz sollte dann eingeschränkt werden und eine Administration über die lokalen Schnittstellen erfolgen, wenn die Erfüllung der Anforderungen an Vertraulichkeit und Integrität der Netzmanagementinformationen nicht gewährleistet werden kann. In diesem Fall ist auf ein zentrales Netzmanagement zu verzichten.

13.1.7 Sichere Konfiguration der aktiven Netzkomponenten

Neben der Sicherheit von Serversystemen und Endgeräten wird die eigentliche Netzinfrastruktur mit den aktiven Netzkomponenten in vielen Fällen vernachlässigt. Gerade zentrale aktive Netzkomponenten müssen jedoch sorgfältig konfiguriert werden. Denn während durch eine fehlerhafte Konfiguration eines Serversystems nur diejenigen BenutzerInnen betroffen sind, die die entsprechenden Dienste dieses Systems nutzen, können bei einer Fehlkonfiguration eines Routers/ Switches größere Teilnetze bzw. sogar das gesamte Netz ausfallen oder Daten unbemerkt kompromittiert werden.

Im Rahmen des Netzkonzeptes (siehe 13.1.4 Entwicklung eines Netzkonzeptes) sollte auch die sichere Konfiguration der aktiven Netzkomponenten festgelegt werden. Dabei gilt es insbesondere Folgendes zu beachten:

- Für Router und Layer-3-Switching muss ausgewählt werden, welche Protokolle weitergeleitet und welche nicht durchgelassen werden. Dies kann durch die Implementation geeigneter Filterregeln geschehen.
- Es muss festgelegt werden, welche IT-Systeme in welcher Richtung über die Router kommunizieren. Auch dies kann durch Filterregeln realisiert werden.
- Sofern dies von den aktiven Netzkomponenten unterstützt wird, sollte festgelegt werden, welche IT-Systeme Zugriff auf die Ports der Switches und Hubs des lokalen Netzes haben. Hierzu wird die MAC-Adresse (Media Access Control) des zugreifenden IT-Systems ausgewertet und auf ihre Berechtigung hin überprüft.

Für aktive Netzkomponenten mit Routing-Funktionalität ist außerdem ein geeigneter Schutz der Routing-Updates erforderlich. Diese sind zur Aktualisierung der Routing-Tabellen erforderlich, um eine dynamische Anpassung an die aktuellen Gegebenheiten des lokalen Netzes zu erreichen. Dabei kann man zwei verschiedene Sicherheitsmechanismen unterscheiden:

- Passwörter
  Die Verwendung von Passwörtern schützt die so konfigurierten Router vor der Annahme von Routing-Updates durch Router, die nicht über das entsprechende Passwort verfügen. Hierdurch können also Router davor geschützt werden, falsche oder ungültige Routing-Updates anzunehmen. Der Vorteil von Passwörtern gegenüber den anderen Schutzmechanismen ist ihr geringer Overhead, der nur wenig Bandbreite und Rechenzeit benötigt.
- Kryptographische Prüfsummen
  Prüfsummen dienen zur Wahrung der Integrität von gültigen Routing-Updates, bzw. Message Authentication Codes schützen vor deren unbemerkten Veränderungen. Dies wird in der Regel bereits durch das Routing Protokoll gewährleistet.

13.1.8 Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

Nachfolgend wird eine methodische Vorgehensweise aufgezeigt, mittels derer eine umfassende Sicherheitsstrategie für ein Client-Server-Netz entwickelt werden kann. Abhängig vom verwendeten Betriebssystem und den eingesetzten Konfigurationen ist für die jeweilige Ausprägung individuell zu entscheiden, welche der beschriebenen Schritte anzuwenden sind.

In der Sicherheitsstrategie muss aufgezeigt werden, wie ein Client-Server-Netz für die jeweilige Organisation sicher aufgebaut, administriert und betrieben wird. Nachfolgend werden die einzelnen Entwicklungsschritte einer solchen Strategie vorgestellt:

1. **Definition der Client-Server-Netzstruktur**
   Im ersten Schritt sind die logische Struktur des Client-Server-Netzes, insbesondere die Zuordnung der Server und der Netz-Domänen festzulegen. Nach Möglichkeit sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beeinträchtigen können. Sofern sich dies jedoch nicht vermeiden lässt, sind verbindliche Regelungen für die Nutzung von Peer-to-Peer-Funktionalitäten zu treffen.
2. **Regelung der Verantwortlichkeiten**
   Ein Client-Server-Netz sollte von geschulten (Netz-)AdministratorInnen nebst StellvertreterInnen sicher betrieben werden. Diese allein dürfen Sicherheitsparameter im Client-Server-Netz verändern. Sie sind z. B. dafür zuständig, auf den Servern den entsprechenden Verantwortlichen Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Vergabe von Datei- und Verzeichnisberechtigungen, die Freigabe der von anderen benötigten Verzeichnisse bzw. Anwendungen, den Aufbau von Benutzergruppen und -accounts sowie die Einstellung der Systemrichtlinien für BenutzerInnen, Zugriffskontrolle und Überwachung vornehmen können. Die Verantwortlichkeiten der einzelnen BenutzerInnen im Client-Server-Netz sind unter Schritt 11 dargestellt.
3. **Festlegung von Namenskonventionen**
   Um die Verwaltung des Client-Server-Netzes zu erleichtern, sollten eindeutige Namen für die Rechner, Benutzergruppen und die BenutzerInnen verwendet werden. Zusätzlich sollten Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden. Sollen keine Rückschlüsse auf den Inhalt eines freigegebenen Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden.
4. **Festlegung der Regeln für Benutzeraccounts**

Vor der Einrichtung von Benutzeraccounts sollten die Restriktionen, die für alle bzw. für bestimmte dieser Accounts gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge.

5. **Einrichtung von Gruppen**
   Zur Vereinfachung der Administration sollten Benutzeraccounts, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen und ggf. weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzeraccounts zugeordnet. Die Benutzeraccounts erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z. B. denkbar, alle MitarbeiterInnen einer Abteilung in einer Gruppe zusammenzufassen. Eine Zuweisung von Benutzerrechten und -berechtigungen an einzelne BenutzerInnen sollte nur erfolgen, wenn dies ausnahmsweise unumgänglich ist.
6. **Festlegung von Benutzerrechten**
   Rechte gestatten den BenutzerInnen die Ausführung bestimmter Aktionen auf dem System. Sie beziehen sich auf das gesamte System, sind keinem speziellen Objekt zugeordnet und können die Berechtigungen für ein Objekt außer Kraft setzen, da ein Recht Vorrang vor allen Datei- und Verzeichnisberechtigungen haben kann.
7. **Festlegung der Vorgaben für Protokollierung**
   Bei der Konfiguration der Protokollierung ist zu beachten, dass ein Mehr an Protokollierung nicht unbedingt auch die Sicherheit des überwachten Systems erhöht. Protokolldateien, die nicht ausgewertet werden oder die aufgrund ihres Umfangs nur mit großem Aufwand auswertbar sind, führen nicht zu einer besseren Kontrolle der Systemabläufe, sondern sind letztlich nutzlos. Aus diesen Gründen sollte die Protokollierung so eingestellt werden, dass sie im Normalfall nur die wirklich bedeutsamen Ereignisse aufzeichnet. Dabei sind selbstverständlich die gesetzlichen Vorgaben, insbesondere die Anforderungen aus dem Datenschutzgesetz, vorrangig zu beachten (vgl. dazu auch 12.5 Protokollierung und Monitoring).
8. **Regelungen zur Datenspeicherung**
   Es ist festzulegen, wo Benutzerdaten gespeichert werden. So ist denkbar, dass Benutzerdaten nur auf einem Server abgelegt werden. Eine Datenspeicherung auf der lokalen Festplatte ist bei diesem Modell nicht erlaubt. Möglich ist aber auch, bestimmte Benutzerdaten nur auf der lokalen Festplatte abzulegen. Nach welcher Strategie verfahren werden soll, muss jeweils im konkreten Einzelfall festgelegt werden. Eine generelle Empfehlung ist hier nicht möglich.
9. **Einrichtung von Projektverzeichnissen**

Um eine saubere Trennung von benutzer- und projektspezifischen Daten untereinander sowie von den Programmen und Daten des Betriebssystems durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse „Projekte“ und „Benutzer“ angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. BenutzerInnen in jeweils eigenen Unterverzeichnissen abgelegt werden.

10. **Vergabe der Zugriffsrechte**
    Es ist festzulegen, welche Verzeichnisse und evtl. welche Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind. Dies gilt analog für die Freigabe von Druckern.
11. **Verantwortlichkeiten für AdministratorInnen und BenutzerInnen im Client-Server-Netz**
    Neben der Wahrnehmung der Netzmanagementaufgaben (siehe Pkt. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen AdministratorInnen im Client-Server-Netz übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

    - die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
    - die Vergabe von Zugriffsrechten,
    - das Hinterlegen und den Wechsel von Passwörtern und
    - die Durchführung von Datensicherungen.

    Auch die EndbenutzerInnen müssen in einem Client-Server-Netz bestimmte Verantwortlichkeiten übernehmen, sofern ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.
12. **Schulung**
    Abschließend muss festgelegt werden, welche BenutzerInnen zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Echtbetrieb aufgenommen werden. Insbesondere die AdministratorInnen sind hinsichtlich der Verwaltung und der Sicherheit des Systems gründlich zu schulen.

Die so entwickelte Sicherheitsstrategie ist zu dokumentieren und im erforderlichen Umfang den BenutzerInnen des Client-Server-Netzes mitzuteilen. Weiters ist sie laufend etwaigen Veränderungen im Einsatzumfeld anzupassen.

13.1.9 Wireless LAN (WLAN)

Drahtlose Netzwerke bzw. so genannte Wireless LAN (WLAN) – Lösungen ergänzen zunehmend LANs. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung und zum anderen sind für deren Aufbau keine aufwendigen Verkabelungsarbeiten notwendig. Die steigende Zahl von portablen Computern (Notebooks, Tablets, Smartphones etc.) unterstreicht die Forderung nach einem WLAN. Sicherheitstechnisch entstehen neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch die Einführung von WLANs die Sicherheit des gesamten lokalen Netzwerkes zu kompromittieren.

Folgende Maßnahmen sind zu beachten, wenn es um die Installation und Konfiguration eines WLANs geht:

- Geeignete Positionierung und Ausrichtung der Zugriffspunkte und Antennen:
  Die Ausstrahlung über die Organisationsgrenzen hinweg soll weitgehend verhindert werden. Der Einsatz von Richtantennen hilft dabei die unbeabsichtigte räumliche Ausstrahlung zu unterbinden.
- Testen des Umkreises:
  Der mögliche Empfang im Umkreis der Organisation muss überprüft werden. Bei unerwünschten Reichweiten müssen entsprechende Gegenmaßnahmen ergriffen werden.
- Deaktivieren des Sendens der Service Set ID:
  Die Service Set ID (SSID) ist der Name des WLANs, über den Clients ein bestimmtes Netz erkennen. Die Bekanntgabe an Knoten, die diese eindeutige SSID nicht kennen, ist zu verhindern, d. h. das Senden der SSID ist zu deaktivieren (auch wenn das eigentlich keine echte Erhöhung der Sicherheit bedeutet).
- Geeignete Verschlüsselungsoptionen aktivieren:
  Verschlüsselungsoptionen wie WiFi Protected Access 2 (WPA2) oder WiFi Protected Access 3 (WPA3) bieten Schutz vor Zugriffen durch Dritte. Es kann auch ein passender „Transition Mode“ aktiviert werden, bei dem für eine Übergangszeit beide Verfahren unterstützt werden. Bei WEP (Wired Equivalent Privacy) wird nur ein einziger, statischer Schlüssel verwendet, d. h. in jeder WLAN-Komponente in einem Netz muss derselbe WEP-Schlüssel eingetragen sein. Weiters sieht WEP kein dynamisches Schlüsselmanagement vor, so dass die Schlüssel manuell administriert werden müssen. **Da WEP-Schlüssel in kürzester Zeit kompromittiert werden können, bietet dieses Verfahren keinen Schutz mehr und darf daher im Unternehmens- und Behördenumfeld oder bei sonstigen Einsatzbereichen mit sensibler Datenübertragung nicht mehr eingesetzt werden.** Bei der Schlüssellänge ist es sinnvoll den Schlüssel mit der größten Länge zu wählen, sofern die verwendeten Endgeräte dies zulassen. Die verwendbaren Schlüssellängen sollten demnach bei der Anschaffung der WLAN-Komponenten bereits berücksichtigt werden. Bei WPA wird TKIP (Temporal Key Integrity Protocol) eingesetzt, das die Nutzung dynamischer kryptographischer Schlüssel statt ausschließlich statischer bei WEP erlaubt. Bei IEEE (Institute of Electrical

and Electronics Engineers) 802.11i (WPA2) kommt zusätzlich CCMP (Counter-Mode/CBC-Mac Protocol) als kryptographisches Verfahren zur Integritätssicherung und zur Verschlüsselung der Nutzdaten hinzu. TKIP und CCMP sind symmetrische Verfahren, alle Kommunikationspartner müssen daher einen gemeinsamen Schlüssel konfiguriert haben. Dieser Schlüssel wird als Pairwise Master Key (PMK) bezeichnet. Der PMK kann über zwei verschiedene Wege auf die beteiligten WLAN-Komponenten gelangen:

- Statische Schlüssel: Der PMK kann (analog zu WEP) manuell als ein statischer Schlüssel, als Pre-Shared Key (PSK) bezeichnet, auf Access Points und Clients konfiguriert werden. Es besteht meist die Möglichkeit den gemeinsamen geheimen Schlüssel auch über Passwörter festzulegen. Diese Passwörter werden über Hash-Funktionen in den PMK umgerechnet. Hat ein solcher PSK eine zu geringe Komplexität (im Sinne der Länge des Schlüssels und der Zufälligkeit der Zeichen), ist er anfällig gegenüber Wörterbuch- bzw. Dictionary-Attacken. Daher sollten diese Passwörter eine hohe Komplexität und eine Länge von mindestens 20 Stellen besitzen. Ab einer gewissen Größe eines WLANs ist das Ausrollen eines neuen Schlüssels mit erheblichen Problemen verbunden. Die Nutzung der PSK ist grundsätzlich in der Kombination mit WPA, WPA2 bzw. WPA3 (bzw. im WPA2/WPA3 Transition Mode der beide Optionen unterstützt, je nach verwendeten Endgeräten im WLAN) möglich, wobei WPA mittlerweile keinen ausreichenden Schutz mehr bietet und daher nichtmehr eingesetzt werden sollte. Bei der Verwendung von WPA2-PSK bzw. WPA3-PSK (auch im Transition-Mode), ist zu empfehlen, die Schlüssel zum Schutz der Kommunikation oder zur Authentisierung regelmäßig zu wechseln.
- Dynamische Schlüssel: Eine höhere Sicherheit bietet ein Mechanismus zur dynamischen Schlüsselverwaltung und -verteilung, der dafür sorgt, dass regelmäßig und insbesondere nach einer erfolgreichen Authentifizierung des WLAN-Clients am Access Point ein neuer Schlüssel (PMK) bereitgestellt wird. Für diese Schlüsselverwaltung und -verteilung greift IEEE 802.11i auf einen anderen Standard zurück und zwar auf IEEE 802.1X. Dieser Standard ist zur portbasierten Netzzugangskontrolle in kabelbasierten Netzen entworfen worden. Grundsätzliche Idee in IEEE 802.1X ist, dass die Freischaltung eines Netzports erst dann erfolgt, wenn der Nutzer sich erfolgreich dem Netz gegenüber authentisiert hat. Die Authentisierung erfolgt also auf Schicht 2. Damit so etwas überhaupt funktioniert, spezifiziert IEEE 802.1X eine Schnittstelle zwischen Client, Netzelement und einem Authentisierungssystem. Diese Schnittstelle basiert auf dem Extensible Authentication Protocol (EAP) und einer Adaptierung dieses Protokolls für die Übertragung auf Layer 2 in LAN (als EAP over LAN, EAPOL bezeichnet). Hand in Hand geht damit die Festlegung einer Funktion zur Schlüsselverwaltung und -verteilung.

Generell sollten in regelmäßigen Abständen, mindestens jedoch vierteljährlich, die Schlüsselinformationen bei allen WLAN-Komponenten ausgetauscht werden. Bei größeren Installationen sollte hierfür eine geeignete Funktion in der zentralen WLAN-Managementlösung enthalten sein, um den Arbeitsaufwand gering zu halten. Der Wechsel der Schlüsselinformationen an allen WLAN-Komponenten sollte bereits während der Planungsphase genau getestet werden, um dadurch eventuell auftretende Schwierigkeiten zu erkennen. Darüber hinaus sind zusätzliche Maßnahmen sinnvoll (z. B. VPN - siehe weiter unten).

- Authentifikation der Knoten:
  Möglichkeiten der Authentifikation der Knoten sind zu aktivieren, etwa nach IEEE 802.1X.
- Einsatz einer zusätzlichen Firewall:
  Eine Firewall zwischen dem Zugriffspunkt und dem eigentlichen Netzwerk kann die Sicherheit erhöhen.
- Direkten Zugriff auf das Intranet über das WLAN sperren:
  Ist der Zugang über WLAN nicht durch starke Methoden der Authentifikation der Knoten und Verschlüsselung gesichert, ist er als RAS (Remote Access Service) anzusehen (vgl. 13.1.10 Remote Access (VPN) - Konzeption).
- Ändern von Standardeinstellungen (Passwörtern):
  Standardeinstellungen der Zugriffspunkte – etwa Service Set ID (SSID), SNMP Community String, Administratorpasswort – sind werksseitig voreingestellt und müssen sofort geändert werden, da die Standardpasswörter AngreiferInnen durchaus bekannt sind (vgl. 9.3.1 Regelungen des Passwortgebrauches).
- MAC-Adressfilterung am Zugriffspunkt:
  Der Zugang zu Zugriffspunkten kann bei vielen Geräten auch über die MAC-Adresse (Media Access Control) kontrolliert werden. Dies sollte nach Möglichkeit genutzt werden.
- Nutzung eines Virtual Private Networks (VPN):
  Im WLAN sollte möglichst ein VPN etabliert werden, wodurch die vertraulichen Inhalte mittels IPsec oder TLS geschützt werden. Dies bietet über WPA3/WPA2/ o.ä. hinausgehend eine Ende-zu-Ende Verschlüsselung.
- Für den Bereich der öffentlichen Verwaltung sind entsprechende Vorgaben und WLAN-Policies der Stabsstelle IKT-Strategie des Bundes (CIO) zu beachten (z. B.: [IKT-WLAN], [IKT-CLWLAN]).

Weiterführende Informationen, speziell aber nicht nur für die Organisationen der öffentlichen Verwaltung, sind den von der Stabsstelle IKT-Strategie des Bundes (CIO) herausgegebenen Empfehlungen zur Verwendung von WLANs ([IKT-WLAN]) zu entnehmen. In Ergänzung zu diesen allgemeine Informationen zu WLANs in der Verwaltung wurde von der Stabsstelle IKT-Strategie des Bundes (CIO) die so genannte „Checkliste WLAN“ [IKT-CLWLAN] veröffentlicht. Diese Erweiterung berücksichtigt aktuelle Weiterentwicklungen und Marktveränderungen im Bereich WLAN. Die darin enthaltene Checkliste ermöglicht ein einfaches und pragmatisches Anwenden der Empfehlungen.

13.1.10 Remote Access (VPN) - Konzeption

Im Folgenden ist mit „Remote Access“ generell jede Art von Fernzugriff auf Geschäftsinformationen (mit z. B. auch Mobile-Computing-Geräten) über ein unsicheres resp. öffentliches Netz gemeint.

Durch Remote Access wird es den BenutzerInnen ermöglicht, sich mit einem lokalen Rechner an ein entferntes Rechnernetz zu verbinden und dessen Ressourcen zu nutzen, als ob eine direkte LAN-Koppelung bestehen würde. Dies wird meist mittels einer VPN-Verbindung zwischen einzelnen IT-Systemen, verschiedenen Standorten einer Institution oder auch zu Kunden erreicht.

> *Die Vernetzung vorhandener Teilnetze mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot, lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Informationsfluss von außen in das zu schützende Netz stattfinden kann, sondern auch in die andere Richtung. Darüber hinaus gefährdet die Möglichkeit remote, d. h. von einem entfernten Rechner aus (z. B. aus dem Internet), Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.*

Ein zu schützendes Teilnetz sollte daher nur dann an ein anderes Netz angeschlossen werden, wenn dies unbedingt erforderlich ist. Dies gilt insbesondere für Anschlüsse an das Internet. Dabei ist auch zu prüfen, inwieweit das zu schützende Netz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muss.

Generell lassen sich für den Einsatz von entfernten Zugängen im Wesentlichen folgende Szenarien unterscheiden:

- das Anbinden einzelner stationärer Arbeitsplatzrechner (z. B. für Telearbeit einzelner MitarbeiterInnen),
- das Anbinden mobiler Rechner (z. B. zur Unterstützung von MitarbeiterInnen im Außendienst oder auf Dienstreise),
- das Anbinden von ganzen LANs (z. B. zur Anbindung von lokalen Netzen von Außenstellen oder Filialen),
- der Managementzugriff auf entfernte Rechner (z. B. zur Fernwartung).

Für diese Szenarien bieten VPN-Technologien eine einfache Lösung: entfernte BenutzerInnen verbinden sich über das Internet mit Hilfe von VPN-Clients mit dem Firmennetz. Alternative Möglichkeiten, die heute nur mehr wenig genutzt werden, sind RAS-Zugänge über Standleitungen oder Modemeinwahl.

Unter dem Gesichtspunkt der Sicherheit sind für entfernte Zugänge folgende Sicherheitsziele zu unterscheiden:

1. Zugangssicherheit:
   Entfernte BenutzerInnen müssen durch das VPN- bzw. RAS-System eindeutig zu identifizieren sein. Ihre Identität muss jeweils durch einen Authentisierungsmechanismus bei jedem Verbindungsaufbau zum lokalen Netz sichergestellt werden. Im Rahmen des Systemzugangs müssen weitere Kontrollmechanismen angewandt werden, um den Systemzugang für entfernte BenutzerInnen reglementieren zu können (z. B. zeitliche Beschränkungen oder Einschränkung auf erlaubte entfernte Verbindungspunkte).
2. Zugriffskontrolle:
   Sind die entfernten BenutzerInnen authentisiert, so muss das System in der Lage sein, ihre Remote-Zugriffe auch zu kontrollieren. Dazu müssen die Berechtigungen und Einschränkungen, die für lokale Netzressourcen durch befugte AdministratorInnen festgelegt wurden, auch für entfernte BenutzerInnen durchgesetzt werden.
3. Kommunikationssicherheit:
   Bei einem Remote-Zugriff auf lokale Ressourcen sollen i. Allg. auch über die aufgebaute VPN- bzw. RAS-Verbindung Nutzdaten übertragen werden. Generell sollen auch für Daten, die über VPN- oder RAS-Verbindungen übertragen werden, die im lokalen Netz geltenden Sicherheitsanforderungen bezüglich Kommunikationsabsicherung (Vertraulichkeit, Integrität, Authentizität) durchsetzbar sein. Der Absicherung der VPN- bzw. RAS-Kommunikation kommt jedoch eine besondere Bedeutung zu, da zur Abwicklung der Kommunikation verschiedene Kommunikationsmedien in Frage kommen, die in der Regel nicht dem Hoheitsbereich des Betreibers des lokalen Netzes zuzurechnen sind.
4. Verfügbarkeit:
   Wird der entfernte Zugang im produktiven Betrieb genutzt, so ist die Verfügbarkeit des Zugangs von besonderer Bedeutung. Der reibungslose Ablauf von Geschäftsprozessen kann bei Totalausfall oder bei Verbindungen mit nicht ausreichender Bandbreite unter Umständen beeinträchtigt werden. Durch die Nutzung von alternativen oder redundanten VPN-(bzw. RAS)Zugängen kann diese Gefahr bis zu einem gewissen Grad verringert werden. Dies gilt insbesondere für entfernte Zugänge, die das Internet als Kommunikationsmedium nutzen, da hier in der Regel keine Verbindungs- oder Bandbreitengarantien gegeben werden.

Ein VPN (RAS)-System besteht aus mehreren Komponenten, die zunächst als Einzelkomponenten abgesichert werden sollten. Zusätzlich zu der Absicherung der Systemkomponenten muss jedoch auch ein VPN (RAS)-Sicherheitskonzept erstellt werden, das sich in das bestehende Sicherheitskonzept eingliedert: das VPN (RAS)-System muss einerseits bestehende Sicherheitsforderungen umsetzen und erfordert andererseits das Aufstellen neuer, VPN (RAS)-spezifischer Sicherheitsregeln.

13.1.10.1 Durchführung einer VPN-Anforderungsanalyse

Bevor eine VPN- (oder RAS-)Verbindung zwischen einzelnen IT-Systemen, verschiedenen Standorten einer Institution oder auch zu Kunden eingerichtet wird, sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hardware- und Softwarekomponenten abzuleiten. Durch das Aufstellen und Durchspielen von Nutzungsszenarien können spezielle Anforderungen an die VPN-Architektur oder die VPN-Komponenten aufgedeckt werden.

Im Rahmen der Anforderungsanalyse sind u. a. folgende Fragen zu klären:

- Festlegung der Geschäftsprozesse: Als erstes muss geklärt werden, für welche Geschäftsprozesse das virtuelle private Netz (VPN) genutzt und welche Informationen darüber kommuniziert werden sollen. Aus den Ergebnissen müssen die benötigten Anforderungen ermittelt und gemäß ihrer Bedeutung für das Unternehmen oder die Behörde priorisiert werden. Neben den Geschäftsprozessen müssen auch die Anwendungen, die die jeweiligen Prozesse unterstützen, betrachtet werden. Hierbei muss auch erfasst werden, welche der betroffenen Anwendungen zeitkritisch oder bandbreitenintensiv sind.
- Festlegung der Anwendungszwecke: Es gibt viele unterschiedliche Nutzungsszenarien für VPNs, wie die Durchführung von Fernwartungstätigkeiten, die Anbindung einzelner Mitarbeiter oder ganzer Standorte. Daher muss geklärt werden, welche Einsatzzwecke unterstützt werden sollen und welche VPN-Typen dafür eingesetzt werden (z. B. Site-to-Site-, End-to-End- und End-to-Site-VPNs).
- Festlegung der BenutzerInnen: Es ist zu klären, welche Arten von BenutzerInnen mit welchen Berechtigungen und welchen Vorkenntnissen das VPN nutzen sollen (z. B. AußendienstmitarbeiterInnen, MitarbeiterInnen auf Dienstreise, MitarbeiterInnen einer Zweigstelle). Dabei ist auch zu klären, wie diese sicher identifiziert und authentisiert werden sollen.
- Regelung von Zuständigkeiten: Auch VPN-Komponenten müssen durch fachkundiges Personal administriert und gewartet werden. Bei der Durchführung einer VPN-Anforderungsanalyse sollte daher festgelegt werden, wer für die Administration und den Betrieb des VPNs zuständig ist - und zwar auf beiden Seiten des VPNs. Im Weiteren muss geklärt werden, wer zu benachrichtigen ist, wenn das VPN ausfällt oder wenn Anzeichen für einen Sicherheitsvorfall entdeckt werden. Hierfür muss Fachpersonal vorhanden sein, das über entsprechendes Wissen verfügt.
- Vertraulichkeit und Integrität: Je nach Schutzbedarf bezüglich der Vertraulichkeit und Integrität werden häufig besondere Anforderungen an das VPN gestellt, die i. Allg. durch zusätzliche Sicherheitsmaßnahmen abgedeckt werden können. In vielen Fällen existieren hierzu übergeordnete Regelungen oder

Richtlinien, die bei der Beschaffung und beim Betrieb von VPN-Komponenten berücksichtigt werden müssen. Um Informationen mit hohem Schutzbedarf bezüglich Vertraulichkeit oder Integrität zu übertragen, empfiehlt es sich, gemäß den [Common Criteria] zertifizierte VPN-Komponenten einzusetzen.

- Verfügbarkeit: Besonders bei einer Standortvernetzung wird häufig gewünscht, dass zu jeder Zeit ausreichend schnell Informationen über das VPN ausgetauscht werden können. Besitzen die betroffenen Anwendungen einen höheren Schutzbedarf bezüglich der Verfügbarkeit, sollte dies bei der Anforderungsanalyse berücksichtigt werden. Erhöhte Anforderungen an die Verfügbarkeit lassen sich bei VPNs nicht immer durch technische Sicherheitsmaßnahmen abdecken, da VPNs oft über Netze aufgebaut werden, die nicht unter der eigenen Kontrolle stehen und somit nicht beeinflusst werden können.
- Beschränkung der Netze: Mit VPNs können verschiedene Netze durch Nutzung einer sicheren Verbindung zu einem logischen Netz zusammengefasst werden. Je nach Konfiguration können dadurch alle IT-Systeme eines Netzes auf alle IT-Systeme oder nur auf bestimmte IT-Systeme der anderen Netze zugreifen. Bei der VPN-Anforderungsanalyse sollte entschieden werden, von wo über das jeweilige VPN auf welches Netz und auf welche IT-Systeme zugegriffen werden darf.
- Auswahl der genutzten Applikationen und -protokolle: Über ein VPN können unterschiedliche Arten von Informationen versendet und empfangen werden. Beispielsweise können E-Mails übertragen, Dateien kopiert oder auf einen Webserver zugegriffen werden. Neben diesen klassischen Diensten kann auch auf einem Terminalserver gearbeitet oder über VoIP telefoniert werden. Es sollte daher festgelegt werden, welche Applikationen über ein VPN genutzt werden dürfen und welche nicht. Es muss nicht nur entschieden werden, welche Applikationen eingesetzt werden dürfen, sondern auch die Protokolle, mit denen die Informationen übertragen werden können. Beispielsweise kann festgelegt werden, dass Netzfreigaben nur über SMB (Server Message Block) statt NFS (Network File System) eingebunden werden dürfen.
- Bandbreite und Verzögerung: Ein VPN ermöglicht es, auf Applikationen in einem entfernten Netz zuzugreifen. Da VPN-Verbindungen oft über ein WAN aufgebaut werden, müssen für zeitkritische Anwendungen spezielle Voraussetzungen berücksichtigt werden, besonders im Hinblick auf die verfügbare Bandbreite und Verzögerungen bei der Übertragung. Dies betrifft beispielsweise Zugriffe auf Terminalserver oder die Telefonie über VoIP. Für die VPN-Anforderungsanalyse sollten die benötigten Bandbreiten, die zulässige Verzögerung sowie gegebenenfalls weitere Qualitätsmerkmale des Netzes berücksichtigt werden.
- Geographische Beschränkungen: Ein VPN kann dazu dienen, dass sich mobile Mitarbeiter von beliebigen Orten unterwegs ins Institutions-LAN einwählen können. Wenn dies aber nicht gewünscht wird, sollte festgelegt werden, von wo auf das LAN zugegriffen werden darf. Dies kann auch technisch unterstützt

werden. Beispielsweise könnte nur der IP-Adressbereich eines oder weniger Provider zugelassen werden. Bei einer Wählverbindung könnte anhand der Ländervorwahl gefiltert werden. Zu beachten ist jedoch, dass diese technischen Zugriffsbeschränkungen nicht absolut zuverlässig sind. Zusätzlich müssen also den BenutzerInnen entsprechende organisatorische Vorgaben gemacht werden.

Diese Punkte müssen nicht zwangsläufig pauschal für die gesamte Institution betrachtet, sondern können auch differenziert auf einzelne Standorte oder Anwendungszwecke angewendet werden. Besonders bei der Vernetzung von mehreren Standorten kommt häufig nicht jeder Liegenschaft die gleiche Priorität zu. An kleine Vertriebsbüros werden beispielsweise meist andere Anforderungen bezüglich Verfügbarkeit gestellt als an Unternehmenszentralen. Ebenso bestehen an End-to-End-VPNs andere Anforderungen als an Site-to-Site-VPNs. Als Lösungsansatz könnten die verschiedenen Anwendungszwecke zum Beispiel bezüglich ihrer Anforderungen an Bandbreite, Verfügbarkeit, Vertraulichkeit, Integrität und Dienstgüte (Quality of Service oder kurz QoS) klassifiziert werden.

Die Anforderungen für die geplanten Szenarien sind zu dokumentieren und mit den NetzadministratorInnen und dem technischen Personal abzustimmen.

13.1.10.2 Entwicklung eines VPN-Konzeptes

Ein VPN-Konzept kann grob in drei Teilbereiche unterteilt werden:

- Organisatorisches Konzept
- Technisches Konzept
- Sicherheitskonzept

Im Folgenden werden jeweils die wesentlichen Fragestellungen aufgezeigt, die im Rahmen der Teilkonzepte beantwortet werden müssen. Je nach konkreter Situation ergibt sich naturgemäß ein speziell auf die jeweiligen organisatorischen und technischen Gegebenheiten zugeschnittener zusätzlicher Abstimmungsbedarf.

Das **organisatorische Konzept** sollte folgende Punkte beinhalten bzw. regeln:

- Es sollten die Verantwortlichkeiten für das jeweilige VPN festgelegt werden (Installation, Verwaltung, Überprüfung, Überwachung). Je nach organisatorischer Struktur müssen die Verantwortlichkeiten existierender Rollen erweitert oder neue Rollen geschaffen werden.
- Es muss festgelegt werden, wie und von wem die Benutzerkonten und die Zugriffsberechtigungen verwaltet und administriert werden (Berechtigungskonzept). Ein per Extranet angebundener Lieferant muss beispielsweise andere Zugriffrechte als eine angebundene Zweigstelle haben. Es empfiehlt sich, für den VPN-Zugang unterschiedliche Benutzergruppen mit verschiedenen Berechtigungen zu definieren. Die Gruppenzugehörigkeit von einzelnen BenutzerInnen sollte durch ein entsprechendes Anforderungsprofil geregelt werden, das festlegt, welche Voraussetzungen für die Mitgliedschaft

in einer Gruppe erfüllt werden müssen. Mögliche Voraussetzungen sind der Einsatzzweck (z. B. Telearbeit bzw. Homeoffice, Außendienst-Tätigkeiten, Wartungsarbeiten), Nachweis bestimmter Kenntnisse (z. B. Teilnahme an Schulungen) und eine Zustimmung durch Vorgesetzte. Wie die Erlaubnis zum entfernten Zugriff reglementiert werden soll, muss jeweils innerhalb der Institution entschieden werden. Oft existieren schon ähnliche Regelungen, z. B. für die Erlaubnis zur Nutzung von Internetzugängen, die dann adaptiert werden können. Die erteilten Zugangs- und Zugriffsberechtigungen müssen dokumentiert und bei Änderungen fortgeschrieben werden.

- Für feste entfernte Standorte (wie Telearbeitsplätze) müssen Anforderungen festgelegt werden, die beschreiben, welchen Ansprüchen (z. B. in Bezug auf Sicherheit und technischer Ausstattung) der entfernte Arbeitsplatz genügen muss, damit von dort VPN-Verbindungen in das LAN der Institution erlaubt werden können. Das Konzept kann eine anfängliche sowie eine periodisch wiederkehrende Überprüfung der Räumlichkeiten und dortigen Technik vorsehen und regeln, wie und durch wen diese erfolgt. Die Betriebsorte von VPN-Clients unterliegen häufig nicht der Kontrolle des LAN-Betreibers und besitzen daher auch ein besonderes Gefährdungspotenzial. Gegenüber stationären Clients kommen bei mobilen Clients weitere Gefährdungen hinzu. Nicht jeder Ort, an dem die technischen Voraussetzungen zum VPN-Verbindungsaufbau vorhanden sind, ist dafür geeignet. Daher müssen Regelungen getroffen werden, von welchen Standorten aus VPN-Verbindungen zum Ziel-LAN aufgebaut werden dürfen. Je nach geplantem Einsatzszenario kann es zweckmäßiger sein, eine Negativliste von besonders ungeeigneten Standorten zu führen. Dazu können z. B. Hotel-Foyers, Hotel-Business-Center oder öffentliche Verkehrsmittel gehören.
- Wird die Sicherheit von VPN-Zugängen verletzt, kann dies unter Umständen die Kompromittierung des gesamten LANs nach sich ziehen. Für die VPN-Administration sollten deshalb Verfahren festgelegt werden, die beschreiben, wie Änderungen an der VPN-Konfiguration durchzuführen sind (Beispiel: Beantragung, Überprüfung der geplanten Konfiguration, Durchführung, Überprüfung der durchgeführten Veränderung).
- Ein weiterer wichtiger Punkt bei der Konzeption ist die grundsätzliche Frage, ob eine Eigenrealisierung bzw. Eigenbetrieb des VPNs notwendig ist oder ob auf Fremdrealisierung bzw. -betrieb zurückgegriffen wird. Viele Dienstleister verfügen über hohe Kompetenz und Erfahrung in Bezug auf die Planung, Einrichtung und den Betrieb von VPNs. Allerdings ist es nicht immer vorteilhaft oder erwünscht, den kompletten Betrieb eines VPNs aus der Hand zu geben. Bei Fremdbetrieb eines VPNs müssen die Anforderungen aus 15.1 Outsourcing beachtet werden.
- Der Schutzbedarf für das VPN muss ermittelt werden. Dieser leitet sich aus dem Schutzbedarf der darüber übertragenen Informationen sowie der damit verbundenen IT-Komponenten ab. In diesem Zusammenhang muss auch ermittelt werden, wie sich eine Nichtverfügbarkeit des Systems auswirkt und

welche Ausfallzeiten hingenommen werden können. Die Anforderungen an die VPN-Sicherheitsmechanismen (z. B. Authentisierung und Integritätssicherung) müssen definiert werden. Hierbei muss hinterfragt werden, ob starke Kryptographie an allen beteiligten Standorten rechtlich eingesetzt werden darf.

- Haben externe Zulieferer oder Kunden eine Anbindung an das VPN, so müssen unterschiedliche Sicherheitszonen definiert werden. Aus den Sicherheitszonen heraus dürfen nur die Zugriffe erlaubt werden, die tatsächlich für die BenutzerInnen erforderlich sind.
- Um einem Missbrauch vorzubeugen, müssen in der VPN-Sicherheitsrichtlinie die Rechte und Pflichten von VPN-BenutzerInnen festgelegt werden. Diese müssen entsprechend verbindlich verpflichtet werden, die Sicherheitsregelungen einzuhalten.
- Da beim entfernten Zugriff auf ein LAN besondere Sicherheitsrisiken durch die meist ungesicherte Umgebung eines VPN-Clients bestehen, sollte alle VPN-BenutzerInnen eine besondere Schulung erhalten. Im Rahmen dieser Schulung sollen die BenutzerInnen einerseits für die spezifischen VPN-Gefährdungen sensibilisiert und andererseits im Umgang mit den technischen Geräten und der Software unterrichtet werden. Falls Authentisierungstoken zum Einsatz kommen sollen, müssen die BenutzerInnen über deren ordnungsgemäße Handhabung informiert werden. Ebenso müssen auch die AdministratorInnen sowohl für die eingesetzten Produkte gründlich ausgebildet als auch über VPN-Sicherheitsrisiken und Sicherheitsmaßnahmen aufgeklärt werden.
- Den AdministratorInnen muss nicht nur für den Betrieb des VPNs ausreichend Zeit zur Verfügung stehen, sondern auch für die Suche nach Informationen über aktuelle VPN-Sicherheitslücken, die Konzeption von Maßnahmen zur Steigerung der Informationssicherheit beim VPN-Betrieb und die Einarbeitung in neue Komponenten.

Das **technische Konzept** sollte folgende Punkte beinhalten bzw. regeln:

- Es sollte beschrieben sein, wie das VPN durch Hardware- und Softwarekomponenten technisch realisiert ist. Die Komponenten werden lediglich durch ihre Funktion definiert. Im Rahmen einer nachgeschalteten Analyse vorhandener Systemkomponenten und am Markt beschaffbarer neuer Komponenten können die Elemente des Konzeptes tatsächlichen Geräten und Softwareprodukten zugeordnet werden.
- Alle potenziellen VPN-Endpunkte, die die Einwahl in das LAN ermöglichen, und die dafür verwendeten Zugangsprotokolle sind zu beschreiben.
- Im Rahmen der Sicherheitskonzeption sind alle VPN-Zugangspunkte zum lokalen Netz zu erfassen und es ist zu beschreiben, wie diese Zugangspunkte an das LAN angeschlossen werden. Das Sicherheitskonzept muss aufbauend auf der aktuellen Netzstruktur analysieren, welche Teilnetze bei Nutzung eines VPN-Zugangs erreichbar sind. Es sollte überlegt werden, dedizierte

Zugangsnetze (Access Networks) zu bilden, aus denen nur kontrolliert (über Router, Paketfilter bzw. interne Firewall) in das produktive Netz zugegriffen werden kann. Die Bildung von Zugangsnetzen erfordert dabei die Anschaffung und Wartung zusätzlicher Hard- und Software.

- Alle Dienste und Protokolle, die über den VPN-Zugang zugelassen werden, sowie die darüber zugreifbaren Ressourcen sind zu dokumentieren. Die Auswahl ist davon abhängig, welche Applikationen eingesetzt werden sollen. Für einen zeitkritischen Datenverkehr werden eventuell QoS (Quality of Service), MPLS (Multi Protocol Label Switching) oder dedizierte Leitungen benötigt.
- Es müssen geeignete Verschlüsselungsverfahren zum Schutz der Daten festgelegt werden. Relevant sind hier unter anderem:
    - Tunneling: Die Kommunikation kann auf niedriger Protokollebene verschlüsselt werden (so genanntes Tunneling). Dazu muss ein geeignetes Verfahren ausgewählt werden. Die herkömmlichen VPNs stellen solche Verfahren standardmäßig, jedoch in unterschiedlicher Zahl und Ausprägung zur Verfügung.
    - TLS-Verschlüsselung: Zur Verschlüsselung kann auch TLS eingesetzt werden, wenn von der Verschlüsselung auf niedriger Protokollebene aus bestimmten Gründen kein Gebrauch gemacht werden kann. Dies gilt besonders für Zugriffe auf Webserver oder E-Mail-Server über Browser, die standardmäßig TLS-gesicherte Kommunikation unterstützen.
    - Verschlüsselung durch Netzkoppelelemente: Neben der Absicherung der Kommunikation durch Software kann auch der Einsatz von verschlüsselnden Netzkoppelelementen (Router, Modems) erwogen werden. Diese sind besonders für den stationären Einsatz und zur Anbindung mehrerer Rechner sinnvoll, da die Verschlüsselung transparent erfolgt und die Endsysteme nicht belastet werden. Zu beachten ist jedoch, dass die Netzkoppelelemente sorgfältig konfiguriert und gewartet werden müssen.
- Es gibt verschiedene Arten von VPNs (Site-to-Site, End-to-End, End-to-Site), anhand der Anforderungen muss entschieden werden, welcher VPN-Typ realisiert werden soll.
- Es muss entschieden werden, ob die Verbindung über dedizierte Carrier-Leitungen realisiert werden muss. Diese Entscheidung hat in der Regel erheblichen Einfluss auf die Kosten.
- Um einen stabilen Betrieb und eine kontinuierliche Verbesserung gewährleisten zu können, sollten geeignete Monitoring-Systeme eingeplant werden. Die aus den Monitoring-Systemen gewonnenen Erkenntnisse tragen wesentlich zur Feinabstimmung des VPN-Betriebs bei.

Das **VPN-Sicherheitskonzept** sollte folgende Punkte beinhalten bzw. regeln:

- Für den Einsatz von VPN-Komponenten in Behörden und Unternehmen müssen geeignete Sicherheitsrichtlinien aufgestellt werden. Diese VPN-spezifischen Sicherheitsrichtlinien müssen konform zum generellen Sicherheitskonzept und den allgemeinen Sicherheitsrichtlinien der Institution sein. Sie müssen regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Die VPN-spezifischen Vorgaben können in den vorhandenen Richtlinien ergänzt oder in einer eigenen Richtlinie zusammengefasst werden.
- Es sollte beschrieben sein, wer in der Institution VPN-Komponenten installieren, konfigurieren und benutzen darf. Dazu sind auch eine Vielzahl von Randbedingungen festzulegen wie z. B.
    - welche Informationen über VPNs übertragen werden dürfen,
    - wo die VPN-Komponenten benutzt werden dürfen,
    - auf welche anderen internen oder externen Netze oder IT-Systeme über ein VPN zugegriffen werden darf.
- Für alle VPN-Komponenten sollten Sicherheitsmaßnahmen und eine Standard-Konfiguration festgelegt werden.
- Alle VPN-BenutzerInnen sollten darauf hingewiesen werden, dass bei einem Verdacht auf Sicherheitsprobleme ein Sicherheitsverantwortlicher hierüber informiert werden muss, damit dieser weitere Schritte unternehmen kann.
- AdministratorInnen, aber auch BenutzerInnen von VPN-Komponenten sollten über VPN-Gefährdungen und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.
- Die korrekte Umsetzung der in der VPN-Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden.
- Um BenutzerInnen nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene VPN-BenutzerInnenrichtlinie zu erstellen, z. B. in Form eines Merkblattes. In einer solchen BenutzerInnenrichtlinie sollten dann kurz die Besonderheiten bei der VPN-Nutzung beschrieben werden, wie z. B.
    - an welche anderen internen und externen Netze oder IT-Systeme der VPN-Client gekoppelt werden darf,
    - unter welchen Rahmenbedingungen sie sich an einem internen oder externen VPN anmelden dürfen,
    - welche Schritte bei (vermuteter) Kompromittierung des VPN-Clients zu unternehmen sind, vor allem, wer zu benachrichtigen ist.
- BenutzerInnen sollten darauf hingewiesen werden, dass VPNs nur von geeigneten Standorten und mit von der Institution dafür zugelassenen IT-Komponenten aufgebaut werden dürfen. Ungeeignete Standorte können je nach Einsatzzweck z. B. Hotel-Foyers, Hotel-Business-Center oder öffentliche Verkehrsmittel sein, fremd-administrierte IT-Systeme können ebenso ungeeignet sein. Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass
    - keine sicherheitsrelevanten Konfigurationen verändert werden dürfen,

    - Passwörter nicht auf dem Client gespeichert werden dürfen, es sei denn mit von dafür freigegebenen Passwort-Speicher-Tools,
    - stets ein Virenscanner aktiviert sein muss,
    - eine vorhandene Personal Firewall nicht abgeschaltet werden darf,
    - die Konfiguration der VPN-Clients nicht von den BenutzerInnen verändert werden darf, sondern nur durch die hierfür benannten AdministratorInnen, und
    - alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind.
- Außerdem sollte die BenutzerInnenrichtlinie Angaben dazu enthalten, welche Daten im VPN genutzt und übertragen werden dürfen und welche nicht. Hierzu gehört vor allem der Umgang mit klassifizierten Informationen, beispielsweise Verschlusssachen. BenutzerInnen sollten für VPN-Gefährdungen sowie für Inhalte und Auswirkungen der VPN-Richtlinie sensibilisiert werden.
- Daneben sollte eine VPN-spezifische Richtlinie für AdministratorInnen erstellt werden, die auch als Grundlage für die Schulung der AdministratorInnen dienen kann. Darin sollte festgelegt sein, wer für die Administration der unterschiedlichen VPN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten AdministratorInnen gibt, und wann welche Informationen zwischen den Zuständigen fließen müssen. So ist es durchaus üblich, dass für den Betrieb der serverseitigen Komponenten eine andere Organisationseinheit zuständig ist als für die Betreuung der VPN-Clients oder für das Identitäts- und Berechtigungsmanagement. Die VPN-Richtlinie für AdministratorInnen sollte weiters die wesentlichen Kernaspekte zum Betrieb einer VPN-Infrastruktur umfassen, wie z. B.
    - Festlegung einer sicheren VPN-Konfiguration und Definition von sicheren Standard-Konfigurationen,
    - geeignete Verwaltung aller VPN-Komponenten,
    - Auswahl und Einrichtung von Kryptoverfahren inklusive Schlüsselmanagement,
    - regelmäßige Auswertung von Protokolldateien, zumindest auf den Servern,
    - Inbetriebnahme von Ersatzsystemen,
    - Maßnahmen bei Kompromittierung des VPNs.
- Alle VPN-AnwenderInnen, egal ob BenutzerInnen oder AdministratorInnen, sollten mit ihrer Unterschrift bestätigen, dass sie den Inhalt der VPN-Sicherheitsrichtlinie gelesen haben und die darin definierten Anweisungen auch einhalten. Ohne diese schriftliche Bestätigung sollte niemand VPNs nutzen dürfen. Die unterschriebenen Erklärungen sind an einem geeigneten Ort, beispielsweise in der Personalakte, aufzubewahren.

Die VPN-Planung muss der Leitungsebene zur Entscheidung vorgelegt werden. Alle Entscheidungen müssen nachvollziehbar dokumentiert werden.

13.1.10.3 Auswahl einer geeigneten VPN-Systemarchitektur

Unternehmen und Behörden haben vielfältige Anforderungen an Netze, wie beispielsweise die Vernetzung unterschiedlicher Standorte und die Anbindung mobiler MitarbeiterInnen oder TelearbeiterInnen an das interne Netz. Dementsprechend unterscheiden sich die Anforderungen der Institutionen und müssen bei der Auswahl von VPN-Produkten berücksichtigt werden.

Typische VPN-Nutzungsszenarien
Nachfolgend werden einige Einsatzszenarien, in denen VPNs üblicherweise eingesetzt werden, beschrieben.

- Mobile MitarbeiterInnen:
  Mobile MitarbeiterInnen arbeiten an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen und benötigen dabei unter Umständen einen Fernzugriff auf Daten im LAN innerhalb der Institution. Neben der Absicherung solcher Verbindungen muss auch die Sicherheit des Endgeräts sowie dessen Einsatzumgebung beachtet werden. Je nach Aufgabengebiet kann es sein, dass sich die MitarbeiterInnen von beliebigen Arbeitsorten, z. B. einem Hotel oder Flughafen, ins interne Netz einwählen möchten. Die Endgeräte der Mitarbeiter sind typischerweise Notebooks, Tablets oder Smartphones.
- Telearbeitsplatz:
  Bei der Anbindung eines Telearbeitsplatzes greift ein Client-System von einem festen Arbeitsort außerhalb der Büroumgebung auf das interne Netz einer Institution zu. Die Kommunikation zwischen Telearbeitsrechner und LAN erfolgt normalerweise über unsichere, öffentliche Netze. Die IT-Systeme des Telearbeitsplatzes sollten zentral administriert werden.
- Standortvernetzung:
  Bei der Standortvernetzung werden Teilnetze an unterschiedlichen Standorten einer Institution miteinander verbunden. Hierbei werden die vertrauenswürdigen LANs, die unter eigener Kontrolle stehen, häufig über ein unsicheres öffentliches Transportnetz verbunden. In diesem Szenario ist besonders der Transportkanal abzusichern. Zusätzlich müssen die Netze und die Client-Systeme der Standorte mittels Sicherheitsgateways gegen Angriffe aus dem Internet gesichert werden.
- Kunden- und Partner-Anbindung:
  Häufig sollen Kunden oder Partner an das interne Netz einer Institution angebunden werden. Folgende Szenarien sind typisch
    - Es sollen bestimmte interne Informationen bereitgestellt werden, so dass diese aus einem nur eingeschränkt vertrauenswürdigen Netz, d. h. von „außen“, abgerufen werden können.

- Aus dem vertrauenswürdigen Netz heraus, d. h. von „innen“, sollen externe Datenbanken abgefragt werden, z. B. um Waren aussuchen und bestellen zu können.
- Auf internen Systemen soll durch externe Firmen Software entwickelt werden.

Da die IT-Systeme der Kunden oder der Partner nicht unter der Kontrolle der Institution stehen, muss gewährleistet werden, dass nur auf die freigegebenen Ressourcen zugegriffen werden kann. Beispielsweise könnten alle IT-Systeme, auf die Kunden oder Partner zugreifen können, in einem separaten Netz betrieben werden, dass mit einem Sicherheitsgateway (Firewall) vom LAN der Institution getrennt ist.

- Fernwartung:
  Bei der Durchführung von Fernwartungstätigkeiten sind privilegierte Administratorzugänge auf interne Systeme erforderlich. Die Fernwartung (Wartung, Support und Betrieb) interner Systeme kann durch eigene oder fremde MitarbeiterInnen durchgeführt werden. In beiden Fällen bestehen hohe Anforderungen an die Authentisierung der entfernten BenutzerInnen, die Datenflusskontrolle und die Verfügbarkeit der Anbindung. Werden fremde MitarbeiterInnen beauftragt, die IT-Systeme zu warten, müssen die Empfehlungen aus 15.1 Outsourcing berücksichtigt werden.

VPNs werden häufig auch verwendet, um die Kommunikation einzelner Protokolle und Anwendungen zu schützen. Unterstützen beispielsweise die vorhandenen WLAN-Komponenten selbst keine sichere Verschlüsselung, könnte die gesamte WLAN-Kommunikation mit einem VPN, das unabhängig vom WLAN ist, verschlüsselt übertragen werden. Die Signalisierung und der Medientransport einer VoIP-Verbindung könnten ebenfalls in einem VPN-Tunnel gebündelt und verschlüsselt werden.

VPN-Endpunkte

Bei den VPN-Endpunkten wird grundsätzlich zwischen VPN-Server und VPN-Client unterschieden. Derjenige Endpunkt, zu dem die Verbindung aufgebaut wird, fungiert als VPN-Server. Der initiierende Endpunkt wird als VPN-Client bezeichnet. VPN-Endpunkte lassen sich entweder per Software oder per Hardware realisieren. Bei MitarbeiterInnen im Außendienst besteht der VPN-Client in der Regel aus einer Softwareapplikation auf einem mobilen IT-System. Ein derartiger VPN-Client greift oft sehr stark in das installierte Betriebssystem ein. Die parallele Installation mehrerer unterschiedlicher VPN-Clients auf einem Endgerät sollte daher vermieden werden. Die Vernetzung der einzelnen VPN-Endpunkte untereinander muss anhand der Ergebnisse der Anforderungsanalyse durchgeführt werden.
Bei den VPN-Endpunkten muss für eine sichere Authentisierung gesorgt werden, damit nur Berechtigte sich über das VPN einwählen können. Hierbei ist, je nach Anwendungsgebiet, auch der Einsatz eines Authentisierungsservers, beispielsweise eines RADIUS-Servers (Remote Authentication Dial In User Service), denkbar.

VPN-Typen

VPNs können eingesetzt werden, um entfernte physische Netze zu einem logischen zusammenzufassen oder um einzelne Endgeräte, die sich in unsicheren Netzen befinden, über einen geschützten Kanal an ein zentrales LAN anzubinden. Je nachdem, welche Systeme den Endpunkt der VPN-Verbindung darstellen, wird zwischen Site-to-Site-, End-to-End- und End-to-Site-VPNs unterschieden.

- Site-to-Site-VPN
  Mit Site-to-Site-VPNs werden Netze gekoppelt, um gemeinsame Anwendungen betreiben bzw. nutzen zu können. Es werden netzübergreifende Zugriffe benötigt. Der Transportkanal wird durch VPN-Gateways in den angeschlossenen Netzen gesichert. Eine typische Verwendung für Verbindungen zwischen LANs ist die Anbindung von Außenstellen oder Filialen an das institutionsinterne Netz.
- End-to-End-VPN
  End-to-End-VPNs werden meist für die Nutzung einzelner Anwendungen verwendet. Die Verbindungen lassen sich auf spezielle Systeme und Dienste beschränken. Typische Verwendungen für End-to-End-VPNs sind:
  - Fernwartung dedizierter Systeme, bei der Zugriffe auf Administratorebene erforderlich sind.
  - Zugriffe auf einzelne Anwendungen oder Datenbanken. Hierbei sind Berechtigungen auf Administrator- bzw. Systemebene häufig nicht erforderlich.
  - Zugriffe über Terminalserver. Durch Fernzugriff auf ein entferntes System können viele dort installierte Anwendungen genutzt werden. Berechtigungen auf Administrator- bzw. Systemebene auf dem Terminalserver sind dafür normalerweise nicht erforderlich.
  - Integration von Geschäftspartnern oder Kunden in Teilbereiche des zentralen Datennetzes einer Institution.
- End-to-Site-VPN (Remote-Access-VPN)
  End-to-Site-VPNs werden auch als Remote-Access-VPN (RAS-VPN) bezeichnet. Solche VPNs werden für Zugriffe eines Clients auf mehrere Anwendungen verwendet, die auf unterschiedlichen IT-Systemen im LAN einer Institution liegen. Dadurch wird Zugriff auf das gesamte Netz benötigt, so dass meist VPN-Software auf dem Client-System und ein VPN-Gateway/-Konzentrator im LAN den Transportkanal sichern. TelearbeiterInnen und mobile BenutzerInnen werden in der Regel mit End-to-Site-VPNs in das LAN integriert.

VPN-Varianten
Der Begriff VPN wird oft als Synonym für verschlüsselte Verbindungen verwendet. VPN-Varianten werden häufig auch nach dem eingesetzten VPN-Protokoll benannt, wie beispielsweise TLS-VPN oder IPsec-VPN. Zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, wie beispielsweise spezielle Funktionen des genutzten Transportprotokolls. Zusätzlich werden zwei grundlegende VPN-Varianten unterschieden: Trusted-VPN und Secure-VPN.

VPNs werden als **Trusted-VPN** bezeichnet, wenn die VPN-Verbindung zwischen verschiedenen Standorten durch vertrauenswürdige externe VPN-Dienstleister gewährleistet wird. Dabei werden die Daten aus dem vertrauenswürdigen Netz in der Regel unverschlüsselt über einen dedizierten Kommunikationskanal zu einem Gateway-Router des Anbieters geleitet. Die Bildung des VPNs erfolgt durch logische Abschottung des VPN-Datenverkehrs vom übrigen Datenverkehr (z. B. mittels Multiprotocol Label Switching, MPLS). Für mobile NutzerInnen stellen Dienstleister zudem VPNs über Gateway-Router bereit, die nur über spezielle Einwahl-Knoten erreicht werden können, die vor unberechtigtem Zugriff geschützt sind.

Wird ein externer Dienstleister beauftragt, ein Trusted-VPN zur Verfügung zu stellen, sollte zusätzlich 15.1 Outsourcing berücksichtigt werden.

Für vertrauliche Daten sind Trusted-VPNs ohne zusätzliche Verschlüsselung auf der Anwendungsschicht nicht geeignet, da die Sicherheit solcher Verbindungen ausschließlich in Händen des VPN-Dienstleisters liegt. So bietet ein Trusted-VPN zum Beispiel keinen Schutz gegen Innentäter des Anbieters. Für die vertrauliche Datenkommunikation empfiehlt sich daher ein Secure-VPN.

Die Abhängigkeit von Dritten in Bezug auf Vertraulichkeit kann vermieden werden, wenn die Kommunikation an den Endpunkten der Verbindung durch Verschlüsselung geschützt wird, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Diese Lösung wird auch als **Secure-VPN** bezeichnet.

Werden für die Realisierung des VPNs dedizierte Carrier-Leitungen eingesetzt, handelt es sich um eine Sonderform eines Trusted-VPNs. Auch in diesem Fall müssen vertrauliche Daten vor der Übertragung durch Verschlüsselung geschützt werden, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Die Verschlüsselung kann an den VPN-Endpunkten auf Transportebene (Secure-VPN) oder auf Anwendungsebene erfolgen.

VPN-Geräte
Grundsätzlich muss eine Entscheidung darüber getroffen werden, ob das gewählte VPN-Produkt ein dediziertes VPN-Gerät, ein Kombi-Gerät oder eine software-basierte VPN-Lösung auf Standard-IT-Systemen (z. B. Linux mit IPsec) sein soll:

- Dedizierte VPN-Gateways (Appliances):
  Diese VPN-Produkte dienen ausschließlich der Realisierung von VPN-Verbindungen und bieten keine darüber hinausgehenden Funktionalitäten, wie beispielsweise Inhaltsfilterung auf Anwendungsebene. VPN-Appliances haben den Vorteil, dass sie für den VPN-Einsatz optimiert sind und die sichere Konfiguration vereinfacht wird, da beispielsweise das Betriebssystem bereits gehärtet ist.
- Kombi-Geräte:

Integrierte VPN-Geräte können beispielsweise Router und andere Komponenten von Sicherheitsgateways (z. B. Application Level Gateways, ALGs) darstellen, die über eine VPN-Funktionalität verfügen oder entsprechend erweitert werden können. Kombi-Geräte haben neben den finanziellen Aspekten oft den Vorteil, dass die unterschiedlichen Funktionalitäten gemeinsam an einer Stelle administriert werden können. Die Kombination verschiedener Funktionalitäten auf einem Gerät kann jedoch zu Lasten der Performance gehen. Bei einer intensiven VPN-Nutzung ist daher zu prüfen, ob aus Gründen der Verfügbarkeit oder des Durchsatzes eigenständige VPN-Komponenten vorzuziehen sind. Manche Kombi-Geräte bieten die Möglichkeit, (auch nachträglich) spezielle Hardwareverschlüsselungsmodule zur Steigerung der Performance einzubauen.

- VPNs auf Basis von Standard-IT-Systemen:
  VPN-Geräte können mit frei verfügbaren oder kommerziellen Softwarekomponenten selbst zusammengestellt werden. Diese Komponenten können oft auf handelsüblicher Hardware mit Standardbetriebssystemen installiert werden. Zusammengestellte VPN-Geräte bieten eine hohe Flexibilität und sind für viele Anwendungsfälle gut geeignet. Die Installation und Integration der benötigten Komponenten kann jedoch fehlerträchtig sein. Daraus können sich Sicherheitsrisiken beim Einsatz eines zusammengestellten VPN-Gerätes ergeben. Ein weiterer Nachteil ist, dass bei Support-Anfragen meist unterschiedliche Ansprechpartner für die einzelnen Komponenten des VPN-Gerätes (z. B. Hardware, Betriebssystem, VPN-Software) kontaktiert werden müssen.

Folgende Sicherheitsgrundfunktionen müssen bei der Auswahl von VPN-Produkten erfüllt werden:

- Identifikation, Authentisierung und Autorisierung:
  Hierunter fallen die Identifikation und Authentisierung von Systemen untereinander, von Systemen gegenüber BenutzerInnen und von BenutzerInnen gegenüber Systemen. Es muss möglich sein, verschiedene Benutzerkennungen mit unterschiedlichen Rechteprofilen einzurichten. Es sollten ausreichend starke anerkannte Authentisierungsverfahren vorhanden sein. Remote-Zugriffe sollten durch eine starke Authentisierung abgesichert werden. Es muss außerdem möglich sein, die festgelegten Zugriffsrechte auf den VPN-Komponenten abbilden zu können.
- Dienstgüte (Quality of Service, QoS):
  Im Zusammenhang mit Netzübergängen ist der Begriff Dienstgüte als Überwachung und Steuerung der Kommunikation zu verstehen, die über ein Sicherheitsgateway erfolgen darf. Ein geeignetes Produkt muss die bei der VPN-Konzeption ermittelten Anforderungen erfüllen können und eine Priorisierung von geschäftskritischen Applikationen ermöglichen.
- Übertragungssicherung:

Zur Übertragungssicherung kommen Funktionen zum Einsatz, welche die Vertraulichkeit und Integrität der Daten sichern. Außerdem muss die Authentizität der Kommunikationspartner gewährleistet werden. Wichtig ist dabei, dass das Produkt sichere kryptographische Mechanismen bietet, die dem Stand der Technik entsprechend. Bei der Planung und Realisierung des VPNs muss außerdem die Integration der VPN-Endpunkte in ein Sicherheitsgateway berücksichtigt werden.

- Schlüsselmanagement:
  Zum Schlüsselmanagement müssen geeignete Funktionen vorhanden sein, um geheime und öffentliche Schlüssel für die kryptographischen Mechanismen verwalten, verteilen und eventuell auch erzeugen zu können. Die ausgewählten Produkte sollten dabei möglichst flexibel sein und eine nahtlose Integration verschiedenster Techniken ermöglichen.

Die nun folgende Liste gibt einen Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden. Neben den hier aufgeführten Kriterien müssen weitere spezifische Anforderungen erarbeitet werden, die aus den geplanten konkreten Einsatzszenarien resultieren.
Allgemeine Kriterien

- Performance und Skalierbarkeit
  - Kann das Produkt den Ansprüchen an die Performance gerecht werden?
  - Bietet das Produkt Funktionen zur Lastverteilung?
  - Können die Produkte die zu übertragenen Informationen komprimieren und dekomprimieren?
  - Kann das Produkt einem zukünftigen Wachstumsbedarf gerecht werden (z. B. durch modularen Systemaufbau, einfaches Einbinden neuer VPN-Server, gemeinsame Benutzerverwaltung für alle VPN-Zugänge)?
- Wartbarkeit
  - Ist das Produkt einfach wartbar?
  - Bietet der Hersteller regelmäßige Software-Updates an?
  - Wird für das Produkt ein Wartungsvertrag angeboten?
  - Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
  - Bietet der Hersteller einen kompetenten technischen Kundendienst (Call-Center, Hotline) an, der in der Lage ist, bei Problemen sofort zu helfen?
- Zuverlässigkeit/Ausfallsicherheit
  - Wie zuverlässig und ausfallsicher ist das Produkt?
  - Bietet der Hersteller auch Hochverfügbarkeitslösungen an?

    - Ist das Produkt im Dauerbetrieb einsetzbar?
- Benutzerfreundlichkeit
    - Lässt sich das Produkt einfach installieren, konfigurieren und nutzen? Genügt das Produkt den geltenden Ergonomievorschriften?
    - Ist insbesondere für den VPN-Client die Benutzerführung so gestaltet, dass auch ungeübte BenutzerInnen damit arbeiten können, ohne Abstriche in der Sicherheit in Kauf nehmen zu müssen (z. B. durch kontextsensitive Hilfen, Online-Dokumentation, detaillierte Fehlermeldungen)?
    - Ist die Nutzung des VPN-Clients so konfigurierbar, dass die BenutzerInnen möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?

Funktion

- Installation und Inbetriebnahme
    - Kann die Installation der VPN-Client-Software automatisiert mit vorgegebenen Konfigurationsparametern erfolgen?
    - Ist die Installation der VPN-Client-Software auch für weniger versierte MitarbeiterInnen durchführbar?
    - Können wichtige Konfigurationsparameter vor Veränderungen durch BenutzerInnen geschützt werden?
    - Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Einsteckkarten, Treiber)?
    - Ist das VPN mit gängigen Systemmanagementsystemen kompatibel?
- Verhalten im Fehlerfall
    - Bleibt die Sicherheit des VPN-Zugangs auch nach einem kritischen Fehler gewährleistet?
    - Kann konfiguriert werden, wie sich das System nach einem kritischen Fehler verhalten soll? Kann z. B. eingestellt werden, dass nach einem kritischen Fehler automatisch ein Neustart durchgeführt oder die AdministratorInnen benachrichtigt werden?
- Administration
    - Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
    - Kann die Administration über eine graphische Benutzeroberfläche erfolgen, die sich intuitiv bedienen lässt? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
    - Wird neben der graphischen Administrationsoberfläche auch eine kommandozeilenbasierte Schnittstelle angeboten?

    - Sind die administrativen Funktionen durch eine adäquate Zugriffskontrolle geschützt?
- Protokollierung
    - Bietet das Produkt geeignete Funktionen zur Protokollierung an?
    - Ist konfigurierbar, wie detailliert die Protokollierung erfolgt und welche Arten von Ereignissen aufgezeichnet werden? Werden durch die Protokollierung alle relevanten Daten erfasst?
    - Ist die Protokollierung in der Weise möglich, dass die Daten nach unterschiedlichen Kategorien erfasst werden können (z. B. verbindungsorientiert, benutzerorientiert, protokollorientiert, dienstorientiert)?
    - Sind die Protokolldaten mit einem Zugriffsschutz versehen?
    - Können die Protokolldaten nicht nur lokal gespeichert werden, sondern auch auf entfernten Rechnern (zentrales Protokoll)? Werden für die entfernte Speicherung gängige Verfahren angeboten, so dass auch Fremdsysteme zur Protokollierung benutzt werden können (z. B. syslog)? Können die Protokolldaten abgesichert übertragen werden?
    - Bietet das Produkt leicht bedienbare Funktionen zur Auswertung der Protokolldaten an?
    - Kann die Protokollierung mit dem eingesetzten Systemmanagementsystem zusammenarbeiten, insbesondere hinsichtlich Übertragungsformat und Übertragungsprotokoll?
    - Bietet das Produkt die Möglichkeit an, beim Auftreten bestimmter Ereignisse die AdministratorInnen zu informieren oder auch geeignete Schutzmaßnahmen automatisch durchzuführen? Beispielsweise ist es oft sinnvoll, ein Benutzerkonto zu sperren, wenn mehrere fehlgeschlagene Authentisierungsversuche in Folge für das jeweilige Benutzerkonto festgestellt werden.
    - Kann die Protokollierung an die spezifischen Bestimmungen des Datenschutzes, die für und in der Institution gelten, angepasst werden?
- Kommunikation und Datenübertragung
    - Unterstützt das VPN-Produkt LAN-seitig alle relevanten Netzwerktechnologien (z. B. Ethernet, ATM)?
    - Unterstützt das VPN-Produkt WAN-seitig alle geplanten Zugangstechnologien (z. B. IP/MPLS, Ethernet, Mobiltelefon, analoge Telefonleitung)?
    - Ist die Anzahl der VPN-Clients, die sich gleichzeitig in den VPN-Server einwählen können, ausreichend?
    - Unterstützt das VPN-Produkt die gängigen Protokolle für den entfernten Zugang über Telekommunikationsnetze (z. B. PPP)?

    - Unterstützt das VPN-Produkt die gängigen Dienstprotokolle für den entfernten Zugriff (z. B. TCP/IP)?
    - Werden für den internetbasierten Zugriff die gängigen Tunnelprotokolle (z. B. L2F (Layer 2 Forwarding), IPsec (Internet Protocol Security), TLS (Transport Layer Security), OpenVPN) unterstützt?
    - Bietet das VPN-Produkt je nach verwendeter Zugangstechnologie zusätzliche, technologieabhängige Mechanismen (z. B. Kanalbündelung, Rückruf des VPN-Clients durch den VPN-Server) an?
- Sicherheit: Kommunikation, Authentisierung und Zugriff
    - Bietet das Produkt geeignete Funktionen zur gesicherten Datenübertragung an?
    - Erfolgt die Absicherung der Kommunikation durch standardisierte Mechanismen?
    - Sind alle verwendeten kryptographischen Verfahren etabliert, und entsprechen sie dem Stand der Technik?
    - Erlaubt die Produktarchitektur eine nachträgliche Installation neuer Sicherheitsmechanismen?
    - Bietet das Produkt geeignete Funktionen zur Authentisierung der BenutzerInnen, bevor ihnen Zugang zu lokalen Ressourcen gewährt wird?
    - Können mehrere Authentisierungsmechanismen miteinander verknüpft werden?
    - Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?
    - Erlaubt das VPN die Nutzung eines oder mehrerer gängiger externer Authentisierungsdienste, z. B. Authenticator-Apps, SecureID, TACACS + (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service)?
    - Ist es möglich, zusätzliche externe Authentisierungsdienste (z. B. MOA-ID) einzubinden?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Produkte dahingehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen entsprechend ihrer Relevanz für die Institution gewichtet werden. Analog kann auch der Erfüllungsgrad einer Anforderung durch das jeweilige Produkt in mehrere Stufen eingeteilt werden. Auf der Grundlage der durchgeführten Produktbewertung kann dann eine fundierte Kaufentscheidung getroffen werden.

Vor der Installation muss überprüft werden, ob die ausgewählten Produkte tatsächlich die Anforderungen ausreichend erfüllen und kompatibel mit den vorgesehenen Technologien sind. Die Auswahl der VPN-Geräte stellt einen wesentlichen Aspekt für den reibungslosen Betrieb eines VPNs dar. Die Entscheidung muss daher gut überlegt sein, da spätere Änderungen oft mit hohen Kosten oder auch mit Sicherheitseinbußen verbunden sind.

13.1.11 Remote Access (VPN) - Implementierung

Mit dem Aufbau eines VPNs kann begonnen werden, sobald die erforderlichen Komponenten dafür beschafft worden sind (vgl. voranstehende Maßnahmen). Grundvoraussetzung für den sicheren VPN-Betrieb ist, dass die Installation und Konfiguration aller Komponenten gewissenhaft erfolgt und sich mit den gewählten VPN-Produkten auch tatsächlich die geforderten Sicherheitsfunktionen umsetzen lassen.

Zusätzlich muss die Sicherheit der IT-Systeme gewährleistet werden, auf denen die VPN-Komponenten eingesetzt werden. Dies betrifft besonders IT-Systeme, auf denen ein Standard-Betriebssystem installiert ist und das als VPN-Endpunkt betrieben wird (Beispiel: Linux-System mit VPN-Unterstützung). Daher sind zunächst die generellen Sicherheitsmaßnahmen für jedes dieser Betriebssysteme umzusetzen, wie sie in den jeweiligen Bausteinen der IT-Grundschutz-Kataloge beschrieben werden. Es gibt auch VPN-Komponenten, bei denen die Konfiguration der Plattform vom Hersteller vorgegeben ist und nicht geändert werden kann (VPN-Appliances). Der Einsatz solcher VPN-Geräte spart einerseits Zeit und es wird im Gegensatz zu einer individuellen Lösung weniger fachkundiges IT-Personal benötigt, z. B. für die Konfiguration des Betriebssystems. Andererseits muss beim Einsatz von Appliances den Vorgaben des Herstellers vertraut werden.

13.1.11.1 Sichere Installation des VPN-Systems

Zusätzlich zu den generellen Sicherheitsmaßnahmen, die für die IT-Komponenten zu beachten sind, sollten im Rahmen der Installation eines VPN-Systems folgende Punkte Beachtung finden:

- Während der Installationsphase sollten weder BenutzerInnen noch Dritte auf das VPN oder Teile davon zugreifen dürfen. Es dürfen in dieser Phase also keine Verbindungen zu anderen Netzen vorhanden sein.
- Es muss sichergestellt werden, dass die Installation aller VPN-Komponenten durch qualifiziertes Personal durchgeführt wird. Dies kann vor allem dann schwierig sein, wenn die zu vernetzenden Standorte geografisch weit voneinander entfernt sind. Beispielsweise muss geklärt werden, ob die nötigen

Personalressourcen für eine VPN-Installation auch in anderen Ländern zur Verfügung stehen. Auch VPN-Endpunkte auf mobilen IT-Systemen, beispielsweise Notebooks von AußendienstmitarbeiterInnen, dürfen nur von qualifiziertem IT-Personal installiert werden.

- Die Installation und Konfiguration der VPN-Komponenten ist zu dokumentieren. Dies kann entweder durch eine separate Installationsdokumentation erfolgen oder aber durch eine Bestätigung, dass die Installation mit den Planungsvorgaben übereinstimmt. Abweichungen von der festgelegten Systemarchitektur (beispielsweise zusätzliche Verbindungen) müssen hierbei begründet und dokumentiert werden. Die Qualität der Dokumentation spielt im Hinblick auf die kontinuierliche Verbesserung des VPNs eine wesentliche Rolle.
- Die korrekte Funktion jeder einzelnen Komponente muss überprüft werden (z. B. durch Funktionsprüfungen bzw. Selbsttests oder Lasttests).
- Bei den eingesetzten Produkten müssen vor der Inbetriebnahme alle aktuellen sicherheitsrelevanten Patches bzw. Firmware-Updates eingespielt werden.
- Für jede sicherheitsrelevante Einstellung muss ein Funktionstest der Sicherheitsmechanismen durchgeführt werden. Beispielsweise sollten die Verschlüsselung der Verbindung sowie die eingesetzten Authentisierungsfunktionen mittels eines Netzanalyse-Tools überprüft werden.
- Bevor das System in den Produktiveinsatz genommen wird, muss es in einer vom Produktivnetz getrennten Umgebung aufgebaut und entsprechend getestet werden. Ebenfalls ist es empfehlenswert, bereits in der Testumgebung Performance-Messungen und einen Testlauf der Schlüsselverteilung durchzuführen. Nach Abschluss der Installation ist die korrekte Funktion des Gesamtsystems zu überprüfen (Abnahme und Freigabe der Installation). Bei allen durchgeführten Tests ist darauf zu achten, dass nur die zum Test befugten Personen Zugriff auf das VPN erhalten.

Ist die grundlegende Installation erfolgt, so kann mit der in der Folge beschriebenen sicheren Konfiguration des VPNs begonnen werden. Diese muss das System in einen sicheren Betriebszustand überführen, damit anschließend der laufende Betrieb aufgenommen werden kann. Für den reibungslosen Betrieb des VPNs sind die in 13.1.12 Sicherer Betrieb des VPN-Systems erwähnten Handlungsweisen essenziell. Die dabei gewonnenen Erkenntnisse und Korrekturmaßnahmen müssen angemessen dokumentiert und in das Feinkonzept eingearbeitet werden.

13.1.11.2 Sichere Konfiguration des VPN-Systems

Alle VPN-Komponenten müssen sorgfältig konfiguriert werden, da es durch eine ungeeignete Konfiguration von VPN-Komponenten zu einem Verlust der Verfügbarkeit des Netzes oder Teilen davon kommen kann. Der Verlust der Vertraulichkeit von Informationen oder der Datenintegrität ist ebenfalls denkbar. Unabhängig davon, ob es sich bei VPN-Komponenten um dedizierte Hardware (Appliances) oder softwarebasierte Systeme handelt, spielt daher die korrekte Konfiguration der beteiligten Komponenten eine wesentliche Rolle. Da ein VPN aus

mehreren Komponenten und deren Konfiguration besteht, ergibt sich eine erhöhte Komplexität der Gesamtkonfiguration. Das Ändern eines Konfigurationsparameters bei einer Komponente kann im Zusammenspiel mit den anderen Komponenten zu Sicherheitslücken, Fehlfunktionen oder Ausfällen führen.

Da die Konfiguration eines VPN-Systems in der Regel Veränderungen unterworfen ist (z. B. durch Personaländerungen, neue Nutzungsszenarien, Systemerweiterungen), kann nicht davon ausgegangen werden, dass es genau eine sichere (und statische) Konfiguration gibt, die einmal eingestellt und nie wieder verändert wird. Vielmehr wird die Konfiguration üblicherweise fortlaufend geändert. Es ist Aufgabe der für das VPN zuständigen AdministratorInnen, dass jeweils nur sichere Versionen der Systemkonfiguration definiert werden und das System von einer sicheren Konfiguration in die nachfolgende sichere Konfiguration überführt wird. Alle Änderungen und die jeweils aktuelle Einstellungen müssen nachvollziehbar dokumentiert sein.

Generell kann zwischen den folgenden Konfigurationskategorien unterschieden werden:

- Die *Default-Konfiguration* ergibt sich durch die vom Hersteller voreingestellten Werte für die Konfigurationsparameter. Die Grundeinstellungen, die vom Hersteller oder Distributor einer VPN-Komponente vorgenommen werden, sind nicht unbedingt auf Sicherheit, sondern auf eine einfache Installation und Inbetriebnahme optimiert. Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Standardpasswörter müssen durch eigene, ausreichend komplexe Passwörter ersetzt werden
- Nach der Installation und vor der Inbetriebnahme muss - ausgehend von der Default-Konfiguration - eine sichere *Anfangskonfiguration* durch die AdministratorInnen eingestellt werden. Hier sollten möglichst restriktive Einstellungen gelten, so dass nur die berechtigten AdministratorInnen Veränderungen vornehmen können, um z. B. eine erste Betriebskonfiguration einzustellen, die das geplante Sicherheitskonzept umsetzt.
- Die sicheren *Betriebskonfigurationen* ergeben sich aus den jeweiligen Konfigurationen im laufenden Betrieb. Hier muss auch regelmäßig überprüft werden, ob neu bekannt gewordene Sicherheitslücken Anpassungen erfordern.
- Schließlich sollten sichere *Notfallkonfigurationen* im Rahmen der Notfallplanung definiert und dokumentiert werden. Sie dienen dazu, auch bei eingeschränkter Betriebsfähigkeit die Sicherheit aufrechtzuerhalten. In der Regel werden durch die Notfallplanung mehrere Notfallsituationen definiert. Es empfiehlt sich, für jede der definierten Situationen eine adäquate Notfallkonfiguration festzulegen. Im einfachsten Fall besteht die Notfallkonfiguration darin, den Zugang zum VPN-System zu sperren.

13.1.12 Sicherer Betrieb des VPN-Systems

VPNs sind aufgrund der übertragenen Daten und der Möglichkeit ins interne Netz einzudringen attraktive Ziele für Angreifer und müssen daher sicher betrieben werden. Voraussetzungen hierfür sind die sichere Installation (vgl. 13.1.11.1 Sichere Installation des VPN-Systems) und Konfiguration (vgl. 13.1.11.2 Sichere Konfiguration des VPN-Systems) der beteiligten Hard- und Softwarekomponenten. Zusätzlich müssen alle organisatorischen Abläufe definiert und umgesetzt worden sein (z. B. Meldewege und Zuständigkeiten). Weiters ist zu beachten, dass die angestrebte Systemsicherheit nur gewährleistet werden kann, wenn auch die physikalische Sicherheit der beteiligten Hardwarekomponenten sichergestellt ist.

Die Sicherheit eines VPN-Systems lässt sich grob in drei Bereiche aufteilen:

- die Sicherheit des VPN-Servers,
- die Sicherheit der VPN-Clients und
- die Sicherheit der Datenübertragung.

Im Umfeld des **Servers** sind folgende Empfehlungen für den sicheren Betrieb zu berücksichtigen:

- Der VPN-Zugang sollte durch den Einsatz von Protokollierungs- und Managementwerkzeugen einer ständigen Überwachung unterliegen.
- Die im Rahmen der Überwachung gesammelten Informationen sollten regelmäßig durch geschulte AdministratorInnen kontrolliert werden. Sie sollten dabei nach Möglichkeit durch eine Software zur Auswertung von Protokollierungsdaten unterstützt werden. Die Bestimmungen des Datenschutzes sind zu beachten.
- Werden Sicherheitsvorfälle festgestellt, so sind sofort die vorher festgelegten Maßnahmen zu ergreifen.
- Damit eine geregelte Benutzerauthentisierung beim VPN-Zugriff möglich ist, muss die Konsistenz der Authentisierungsdaten sichergestellt sein. Dies kann durch zentrale Verwaltung der Daten (Authentisierungsserver) oder durch periodischen Abgleich geschehen.
- Für jede Verbindungsaufnahme ist immer die Benutzerauthentisierung über den gewählten Mechanismus durchzuführen.
- Für jede Verbindung sollte die Absicherung der Kommunikation durch eines der im VPN-Sicherheitskonzept erlaubten Verfahren erzwungen werden, damit die übertragenen Daten geschützt sind.
- Revision: Das VPN-System sollte in regelmäßigen Abständen einer Revision unterzogen werden. Die Rollen Administrator und Revisor dürfen nicht der gleichen Person zugeordnet werden.

Da VPN-Clients in der Regel in nicht vollständig kontrollierten Umgebungen betrieben werden, müssen für diesen Fall spezielle Mechanismen, Verfahren und Maßnahmen zum Einsatz kommen, die den Schutz des Clients gewährleisten können. Insbesondere mobile Clients sind hier einer besonderen Gefahr ausgesetzt, da diese physikalisch besonders leicht anzugreifen sind (Diebstahl, Vandalismus). Ist ein Client kompromittiert, so besteht die Gefahr, dass dadurch auch die Sicherheit des LANs beeinträchtigt wird.

Für den sicheren Betrieb von **VPN-Clients** sind daher folgende Aspekte zu berücksichtigen:

- Die Grundsicherheit des IT-Systems muss gewährleistet sein.
- Da mobile VPN-Clients größeren Risiken ausgesetzt sind als stationäre, sollten sie durch zusätzliche Maßnahmen gesichert werden. Hierzu bietet sich eine Festplattenverschlüsselung an, um sicherzustellen, dass von abhanden gekommenen Geräten weder Daten ausgelesen noch unbefugt eine VPN-Verbindung aufgebaut werden kann.
- Insbesondere beim Zugriff über Internetverbindungen ist die Installation von Virenschutzprogrammen auf allen VPN-Clients notwendig.
- Es sollte überlegt werden, auf den VPN-Clients so genannte PC-Firewalls einzusetzen und so vor unberechtigten Zugriffen aus dem Internet durch Dritte zu schützen. Ähnlich wie herkömmliche Firewalls (siehe 13.1.13 Entwicklung eines Firewallkonzeptes ff.) filtern PC-Firewalls die Pakete der Netzkommunikationsprotokolle. Die Filterregeln können jedoch meist dynamisch durch die BenutzerInnen erzeugt werden. Hierzu wird bei jedem Zugriff, für den noch keine Regel vorliegt, eine Auswahl an möglichen Reaktionen (z. B. erlauben, ablehnen, bedingte Verarbeitung) angeboten, um eine neue Regel zu definieren. Da es für die BenutzerInnen jedoch in vielen Fällen schwierig ist, zwischen erlaubten und unberechtigten Zugriffen zu unterscheiden, sollte der Regelsatz durch die AdministratorInnen vorinstalliert werden.
- Auch VPN-Clients sollten in das Systemmanagement einbezogen werden, soweit dies möglich ist. Dies erlaubt einerseits die Überwachung der Clients im Rahmen der Aufrechterhaltung des laufenden Betriebes. Andererseits können so einfach Software-Updates (Virendatenbanken, Anwendungsprogramme) auf geregeltem Weg eingespielt werden. Entfernte Rechner stellen jedoch erhöhte Anforderungen an das Systemmanagement, da diese nicht permanent mit dem Netz der Organisation verbunden sind, so dass die Rechner regelmäßig auf (unzulässige) Konfigurationsveränderungen untersucht werden müssen.
- Falls TCP/IP als Protokoll verwendet wird, sollte überlegt werden, für VPN-Clients feste IP-Adressen zu benutzen und diese nicht dynamisch zu vergeben. Dieses Vorgehen bedeutet zwar einen höheren administrativen Aufwand (Wartung der Zuordnungstabellen), erlaubt jedoch eine eindeutige Zuordnung von Netzadresse und Rechner. Der Nachteil bei einer dynamischen Vergabe

der Netzadressen besteht darin, dass protokolliert werden muss, welchem VPN-Client zu welchem Zeitpunkt eine bestimmte Netzadresse zugewiesen wurde. Anderenfalls ist es meist nicht möglich festzustellen, welcher VPN-Client eine bestimmte Aktion ausgeführt hat.

Die **Kommunikationsverbindung** zwischen VPN-Client und VPN-Server wird in der Regel über Netze von Dritten aufgebaut. Die dabei benutzten Netzkomponenten unterliegen meist nicht der Kontrolle durch den Betreiber des LANs, mit dem die Verbindung aufgebaut werden soll. Es muss weiter davon ausgegangen werden, dass die Daten nicht nur über das Telekommunikationsnetz eines Anbieters übertragen werden, sondern dass auch die Netze von Kooperationspartnern des Telekommunikationsanbieters benutzt werden. Dies gilt insbesondere beim Zugriff auf ein LAN aus dem Ausland. Um dem Schutzbedarf der so übertragenen Daten gerecht zu werden, müssen Sicherheitsmaßnahmen getroffen werden, die z. B. die Vertraulichkeit der Daten sicherstellen. Daher gilt für die Datenübertragung:

- Die Nutzung der Datenverschlüsselung für alle übertragenen Daten ist für den sicheren Betrieb zwingend erforderlich.
- Es sollten Signaturmechanismen eingesetzt werden, um die Authentizität und Integrität der Daten sicherzustellen.

Um diesen Anforderungen an den Schutz der Daten gerecht zu werden, können verschiedene Sicherungsmechanismen für VPN-Verbindungen benutzt werden. Relevant sind hier unter anderem:

- Tunneling:
  Die Kommunikation kann auf niedriger Protokollebene verschlüsselt werden (so genanntes Tunneling, siehe auch 9.4.2 Einsatz geeigneter Tunnelprotokolle für die VPN-Kommunikation). Dazu muss ein geeignetes Verfahren ausgewählt werden. Die herkömmlichen VPN-Systeme stellen solche Verfahren (z. B. IPsec) standardmäßig, jedoch in unterschiedlicher Zahl und Ausprägung zur Verfügung.
- TLS-Verschlüsselung:
  Zur Verschlüsselung kann auch TLS eingesetzt werden, wenn von der Verschlüsselung auf niedriger Protokollebene aus bestimmten Gründen kein Gebrauch gemacht werden kann. Dies gilt besonders für Zugriffe auf Webserver oder E-Mail-Server über Clients, die standardmäßig TLS-gesicherte Kommunikation unterstützen.
- Verschlüsselung durch Netzkoppelelemente:
  Neben der Absicherung der Kommunikation durch Software kann auch der Einsatz von verschlüsselnden Netzkoppelelementen (Routern, Modems) erwogen werden. Diese sind besonders für den stationären Einsatz und zur Anbindung mehrerer Rechner sinnvoll, da die Verschlüsselung transparent erfolgt und die Clients und Server nicht belastet werden. Zu beachten ist jedoch, dass die Geräte sorgfältig konfiguriert und gewartet werden müssen.
- E-Mail-Verschlüsselung:
  Für den Austausch von E-Mails über unsichere Kanäle kann die Nutzung von E-Mail-Verschlüsselung sinnvoll sein.

13.1.13 Entwicklung eines Firewallkonzeptes

IT-Systeme, die zeitweise oder dauernd an Produktionsnetze angeschlossen sind, dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit Fremdnetzen verbunden werden. Diese Sicherheitseinrichtungen, die i. Allg. aus einem zwei- oder mehrstufigen System bestehen, werden als „Firewalls“ bezeichnet.

Um die Sicherheit des zu schützenden Netzes zu gewährleisten, muss eine geeignete Firewall eingesetzt werden. Damit eine Firewall effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein.

Die Firewall muss

- auf einer umfassenden Sicherheitspolitik aufsetzen (vgl. 14.7.2 Erstellung einer Internetsicherheitspolitik),
- in der IT-Sicherheitspolitik und dem IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Der Anschluss an ein Fremdnetz darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten Firewallkonzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Die Aufgaben und Anforderungen an die Firewall müssen in der Internetsicherheitspolitik festgelegt werden.

Damit eine Firewall einen wirkungsvollen Schutz eines Netzes gegen Angriffe von außen bietet, müssen einige grundlegende Voraussetzungen erfüllt sein:

- Jede Kommunikation zwischen den beiden Netzen muss ausnahmslos über die Firewall geführt werden. Dafür muss sichergestellt sein, dass die Firewall die einzige Schnittstelle zwischen den beiden Netzen darstellt. Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen.
- Eine Firewall darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden, daher dürfen auf einer Firewall nur die dafür erforderlichen Dienste verfügbar sein und keine weiteren Dienste wie z. B. ein Webserver, angeboten werden.
- Ein administrativer Zugang zur Firewall darf nur über einen gesicherten Weg möglich sein, also z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz. Eine Konsole sollte in einem Serverraum aufgestellt sein.

- Eine Firewall baut auf einer für das zu schützende Netz definierten Sicherheitspolitik auf und gestattet nur die dort festgelegten Verbindungen. Diese Verbindungen müssen gegebenenfalls sehr detailliert (bis hin zu einer individuellen Angabe von IP-Adresse, Dienst, Zeit, Richtung und BenutzerIn getrennt) festgelegt werden können.
- Jede Sicherheitspolitik muss konzeptionell auf bestmögliche Reduktion des eventuellen Schadensfalles ausgelegt sein (Betrieb von Teilnetzen, frühzeitiger Einsatz von Routern, …). In diesem Zusammenhang ist auch der Raum, in dem die Firewall betrieben wird, zusammen mit den Netzwerkeinrichtungen (wie z. B. Routern) einer besonderen Zugangskontrolle zu unterwerfen (vgl. 11.1.4 Zutrittskontrolle und 11.5.6 Serverräume).
- Es ist zu entscheiden, ob besonders sensible Daten im Netz besser und kostengünstiger durch organisatorische als durch technische Maßnahmen geschützt werden sollen.
- Für die Konzeption und den Betrieb einer Firewall muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb einer Firewall darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Firewall-AdministratorInnen müssen fundierte Kenntnisse über die eingesetzten IT-Komponenten besitzen und auch entsprechend geschult werden.
- Das Firewallkonzept muss sich permanent an Betriebserfahrungen der Firewall sowie aktuellen Entwicklungen orientieren und bei Bedarf unverzüglich angepasst werden.
- Die BenutzerInnen des lokalen Netzes sollten durch den Einsatz einer Firewall möglichst wenig Einschränkungen hinnehmen müssen.

Eine Firewall kann das interne Netz vor vielen Gefahren beim Anschluss an das Internet schützen, aber nicht vor allen. Beim Aufbau einer Firewall und der Erarbeitung einer Firewall-Sicherheitspolitik sollte man sich daher die Grenzen einer Firewall verdeutlichen:

- Es werden Protokolle überprüft, nicht die Inhalte. Eine Protokollprüfung bestätigt beispielsweise, dass eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich.
- Sobald BenutzerInnen eine Kommunikation über eine Firewall herstellen dürfen, können sie über das verwendete Kommunikationsprotokoll beliebige andere Protokolle tunneln. Damit könnten InnentäterInnen Externen den Zugriff auf interne Rechner ermöglichen.
- Eine Einschränkung der Internetzugriffe auf festgelegte Webserver ist in der Realität unmöglich, da zu viele Webserver auch als Proxies nutzbar sind, so dass eine Sperrung bestimmter IP-Adressen leicht umgangen werden kann.
- Die Filtersoftware ist häufig noch unausgereift. Beispielsweise ist es möglich, dass nicht alle Arten der Adressierung erfasst werden. Zudem können URL-Filter durch Nutzung von „Anonymizern“ umgangen werden.

- Die Filterung von Spam-E-Mails ist noch nicht 100 % ausgereift. Keine Firewall kann zweifelsfrei feststellen, ob eine E-Mail vom Empfänger erwünscht ist oder nicht. Spam-E-Mails dürften erst dann verschwinden, wenn die Absender zweifelsfrei nachweisbar sind. Dies ist aber mit dem herkömmlichen Protokoll SMTP alleine nicht realisierbar.
- Firewalls schützen nicht vor allen Denial-of-Service-Attacken. Wenn AngreiferInnen z. B. die Anbindung zum Provider lahm legt, kann auch die beste Firewall nicht helfen. Außerdem gibt es immer wieder Implementationsfehler von Protokollen auf Endgeräten, die eine Firewall nicht abfangen kann.
- Leider ermöglichen viele Firewalls es nicht, durch Hintereinanderschaltung von verschiedenen Firewalls eine erhöhte Sicherheit zu erlangen. Gerade in größeren Firmen ist dies problematisch, wenn innerhalb der Firma Firewalls z. B. auch zur Bildung von abgesicherten Teilnetzen eingesetzt werden.
- Eine Firewall kann zwar einen Netzübergang sichern, sie hat aber keinen Einfluss auf die Sicherheit der Kommunikation innerhalb dieser Netze!
- Auch die speziell unter Sicherheitsaspekten entwickelten Komponenten von Firewalls können trotz großer Sorgfalt Programmierfehler enthalten.
- Firewalls können nur begrenzt gegen eine absichtliche oder versehentliche Fehlkonfiguration der zu schützenden Clients und Server schützen.
- Eingebaute Hintertüren in der verwendeten Software können eventuell auch durch eine Firewall hindurch ausgenutzt werden. Im Extremfall kann die Software der Firewall selbst Hintertüren enthalten.
- Die korrekte Konfiguration der Komponenten der Firewall ist oft sehr anspruchsvoll. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen.
- Ist die Dokumentation der technischen Ausstattung der Firewall durch den Hersteller mangelhaft, so begünstigt dies Fehler bei Konfiguration und Administration.
- Wenn die Komponenten der Firewall falsch dimensioniert sind, kann die Verfügbarkeit beeinträchtigt werden. Wird beispielsweise der Rechner, auf dem ein HTTP-Sicherheitsproxy läuft, zu schwach dimensioniert (zu wenig Arbeitsspeicher, zu langsamer Prozessor), so kann dies die Geschwindigkeit des Internetzugriffes stark beeinträchtigen.
- Es kann nicht verhindert werden, dass Angreifer die Komponenten der Firewall mit Hilfe von Schwachstellenscannern analysieren.
- Eine Firewall kann nicht gegen die bewusste oder unbewusste Missachtung von Sicherheitsrichtlinien und -konzepten durch die Anwender schützen.
- Eine Firewall schützt nicht vor dem Missbrauch freigegebener Kommunikation durch Innentäter („Insider-Angriffe“).
- Eine Firewall schützt nicht vor Social Engineering.

- Werden mobile Endgeräte (Notebook, Smartphone etc.), die von Mitarbeitern auch extern benutzt werden, an das interne Netz angeschlossen, so kann auf diese Weise Schadsoftware (Viren, Würmer, Trojanische Pferde) in das vertrauenswürdige Netz eingeschleppt werden.
- Eine Firewall schützt auch nicht davor, dass Schadprogramme auf Austauschmedien, z. B. externe Festplatten, SD-Karten, USB-Stick, …, in das vertrauenswürdige Netz eingeschleppt werden.

13.1.14 Installation einer Firewall

Bei der Installation einer Firewall sind folgende Schritte in der angegebenen Reihenfolge zu setzen (vgl. [KIT S04]):

1. Festlegen der Sicherheitspolitik sowie der Benutzungsordnung durch organisatorisch und technisch Verantwortliche in Zusammenarbeit mit BenutzervertreterInnen (vgl. auch 7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen)
2. Bestimmung der Sicherheitsverantwortlichen (Datenschutzbeauftragte/CISOs) - soweit nicht bereits nominiert - und Informationssicherheitskoordinatoren im Bereich
3. Definition der angebotenen und anzufordernden Dienste
4. Analyse der Hard- und Softwarevoraussetzungen im internen Netz
5. Auswahl geeigneter Produkte
6. Installation und Konfiguration der Firewall
   Der administrative Zugang zur Sicherheitseinrichtung darf nur über einen gesicherten Weg möglich sein.
7. Überprüfung der Installation durch Querlesen der Definitionen und Funktionskontrolle
8. Dokumentation der Installation zum Zweck der Nachvollziehbarkeit, der Wartung und der Validierung
9. Laufende Beobachtung und Wartung
10. Periodische Sicherheitsüberprüfung durch befugte Externe zu nicht angekündigten Zeitpunkten mindestens einmal im Quartal („Screening“, vgl. 13.1.15 Sicherer Betrieb einer Firewall) sowie Weitermeldung der erhobenen Fakten an die Vorgesetzten
11. Revision der Behebung der bei den Sicherheitstests erhobenen Mängel
12. Sammlung der relevanten Projekterfahrungen als Grundlage für eine Weiterentwicklung der Internetsicherheitspolitik und des Firewallkonzeptes. Im Bereich der öffentlichen Verwaltung sollten diese Projekterfahrungen an die IKT-Koordinierungsstelle weitergegeben werden.
13. Aus- und Weiterbildung des administrierenden Personals

13.1.15 Sicherer Betrieb einer Firewall

Für einen sicheren Betrieb einer Firewall sind eine fachgemäße Administration sowie eine regelmäßige Überprüfung auf die korrekte Einhaltung der umgesetzten Sicherheitsmaßnahmen (Screening) erforderlich.

Insbesondere müssen die für den Betrieb der Firewall getroffenen organisatorischen Regelungen regelmäßig oder zumindest sporadisch auf ihre Einhaltung überprüft werden. Es sollte in zyklischen Abständen kontrolliert werden, ob neue Zugänge unter Umgehung der Firewall geschaffen wurden. Alle Sicherheitskontrollen sollten zumindest teilweise auch durch Externe vorgenommen werden.

Administration

Die Administration einer Firewall umfasst die nachfolgend angeführten Aufgaben:

- Anlegen und Entfernen von BenutzerInnen, Profilen, Filtern etc.,
- Ändern von Berechtigungen, Funktionen etc.,
- Kontrolle und Auswertung der Logfiles,
- Einschränken und Beenden des Internetzugangs,
- Weiterleitung sicherheitsrelevanter Beobachtungen an die in der Sicherheitspolitik definierten Instanzen,
- Benachrichtigung der zuständigen Instanzen bei Entdecken von Angriffen aus dem Internet,
- Verfolgen der aktuellen Entwicklungen im Bereich Sicherheit (z. B. durch Lesen der entsprechenden Newsletter) sowie entsprechende Weiterbildung.

Durch eine angemessene Stellvertreterregelung (und eine entsprechende Schulung der StellvertreterInnen) ist eine kontinuierliche Administration zu gewährleisten.

Regelmäßige Überprüfung

Zusätzlich zu den regelmäßigen Wartungsaktivitäten ist es erforderlich, eine Firewall regelmäßig (etwa einmal pro Quartal) durch eine geeignete Instanz kontrollieren zu lassen. Sicherheitsrelevante Änderungen erfordern zusätzlich „ad hoc“-Kontrollen. Diese Kontrollen sollten vorzugsweise durch eine vertrauenswürdige externe Instanz erfolgen, da die Gefahr besteht, dass Firewall-AdministratorInnen durch Gewöhnungseffekte und Routinearbeit bestimmte Sicherheitslücken übersehen könnten, die neutralen BeobachterInnen mit hoher Wahrscheinlichkeit auffallen. (Vgl. auch Screening, Security Compliance Checking)

Eine derartige Prüfung ist wie folgt durchzuführen:

- Überprüfung der Installation von außen,
- interne Überprüfung der Internetsicherheitspolitik,
- interne Überprüfung der Konfiguration,
- interne Durchführung eventuell notwendiger Korrekturen,

- erneute Prüfung von außen.

Dabei sind die folgenden Punkte zu beachten:

- Alle Filterregeln müssen korrekt umgesetzt sein. Dabei ist zu testen, dass nur die Dienste zugelassen werden, die in der Sicherheitspolitik vorgesehen sind.
- Die Defaulteinstellung der Filterregeln und die Anordnung der Komponenten müssen sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Firewall-Komponenten gelten.
- Es muss die Regel „Alles, was nicht ausdrücklich erlaubt ist, ist verboten“ realisiert sein. So dürfen z. B. BenutzerInnen, die keinen Eintrag in einer Access-Liste haben, keine Möglichkeit haben Dienste des Internets zu benutzen.
- Um ein Mitlesen oder Verändern der Authentisierungsinformationen zu verhindern, dürfen sich AdministratorInnen und Revisor nur über einen vertrauenswürdigen Pfad authentisieren. Dies könnte z. B. direkt über die Konsole, eine verschlüsselte Verbindung oder ein separates Netz erfolgen.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden. Im Fehlerfall ist die Firewall abzuschalten.
- Die Firewall muss auf ihr Verhalten bei einem Systemabsturz getestet werden. Insbesondere darf kein automatischer Neustart möglich sein, und die Access-Listen müssen auf einem schreibgeschützten Medium speicherbar sein. Die Access-Listen sind die wesentlichen Daten für den Betrieb der Firewall und müssen besonders gesichert werden, damit keine alten oder fehlerhaften Access-Listen bei einem Neustart benutzt werden, der durch AngreiferInnen provoziert wird.
- Bei einem Ausfall der Firewall muss sichergestellt sein, dass in dieser Zeit keine Netzverbindungen aus dem zu schützenden Netz heraus oder zu diesem aufgebaut werden können.
- Auf den eingesetzten Komponenten dürfen nur Programme, die für die Funktionsfähigkeit der Firewall nötig sind, vorhanden sein. Der Einsatz dieser Programme muss ausführlich dokumentiert und begründet werden. Beispielsweise sollten die Software für die graphische Benutzeroberfläche sowie alle Treiber, die nicht benötigt werden, entfernt werden. Diese sollten auch aus dem Betriebssystem-Kern entfernt werden. Das Verbleiben von Software muss dokumentiert und begründet werden.
- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb der Firewall relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

Falls nachträgliche Änderungen der Sicherheitspolitik erforderlich sind, müssen diese streng kontrolliert und insbesondere auf Seiteneffekte überprüft werden.

13.1.16 Firewalls und aktive Inhalte

Eines der größten Probleme bei der Konzeption einer Firewall ist die Behandlung der Probleme, die durch die Übertragung aktiver Inhalte zu den Rechnern im zu schützenden Netz entstehen. Hierunter fällt nicht nur die Erkennung und Beseitigung von Viren, die verhältnismäßig einfach auch auf den Rechnern der AnwenderInnen durchgeführt werden kann, sondern auch das weit schwieriger zu lösende Problem der Erkennung von aktiven Inhalten (z. B. JavaScript) mit einer Schadfunktion.

Die Kontrolle aktiver Inhalte kann auf verschiedene Weise geschehen. Eine der Möglichkeiten ist die Filterung durch eine Firewall. Siehe dazu: 12.3.11 Schutz vor aktiven Inhalten.

13.1.17 Firewalls und Verschlüsselung

Da im Internet die Daten über nicht vorhersagbare Wege und Knotenpunkte verschickt werden, sollten die zu versendenden Daten möglichst nur verschlüsselt übertragen werden. Hierbei wäre es sinnvoll, wenn entsprechende Mechanismen schon in den unteren Schichten des Protokolls vorgesehen würden.

Zunächst sollte aber unterschieden werden zwischen

- Verschlüsselung auf der Firewall bzw. auf Netzkoppelelementen, die zum Aufbau sicherer Teilnetze eingesetzt werden, und
- Verschlüsselung auf den Endgeräten, die z. B. von BenutzerInnen bedarfsabhängig eingesetzt wird.

Verschlüsselung auf der Firewall:

Um mit externen Kommunikationspartnern Daten über ein offenes Netz auszutauschen und /oder diesen Zugriff auf das eigene Netz zu geben, kann der Aufbau von virtuellen privaten Netzen (VPNs) sinnvoll sein. Dafür sollten alle Verbindungen von und zu diesen Partnern verschlüsselt werden, damit Unbefugte keinen Zugriff darauf nehmen können. Zum Aufbau von verschlüsselten Verbindungen können eine Vielzahl von Hard- und Softwarelösungen eingesetzt werden. Sollen hierbei nur wenige Liegenschaften miteinander verbunden werden, sind insbesondere Hardwarelösungen basierend auf symmetrischen kryptographischen Verfahren eine einfache und sichere Lösung.

Die Ver- bzw. Entschlüsselung kann auf verschiedenen Geräten erfolgen. So könnte eine Hardwarelösung im Paketfilter als Schlüsselgerät arbeiten. Dies ist insbesondere dann sinnvoll, wenn keine unverschlüsselte Kommunikation über dieses Gerät gehen soll. Die Integration der Verschlüsselung auf dem Application-Gateway hat dagegen den Vorteil einer leichteren Benutzerverwaltung. Zudem können AngreiferInnen, die einen externen Informationsserver unter ihre Kontrolle gebracht haben, die verschlüsselte Kommunikation nicht belauschen.

Verschlüsselung auf den Endgeräten:

Zum Schutz der Vertraulichkeit bestimmter Daten, insbesondere bei der Versendung von E-Mails, bietet sich auch der Gebrauch von Mechanismen an, die eine Ende-zu-Ende-Verschlüsselung ermöglichen. Hierfür wird zum Beispiel häufig das frei verfügbare Programmpaket PGP (Pretty Good Privacy) eingesetzt. Für eine vertrauenswürdige Datenübertragung mit ausgewählten Partnern im Internet sollten Programme wie SSH oder SFTP eingesetzt werden, die eine Verschlüsselung der übertragenen Daten (z. B. mittels TLS) unterstützen.

Die Verschlüsselung auf den Endsystemen wird auf absehbare Zeit noch applikationsgebunden sein, z. B. durch den Einsatz von S/MIME (Secure/ Multipurpose Internet Mail Extensions), TLS oder PGP. Die Verschlüsselung von Daten stellt andererseits aber auch ein großes Problem für den wirksamen Einsatz von Firewalls dar, d. h. den Filtern. Wenn die Übertragung verschlüsselter Daten über die Firewall zugelassen wird (z. B. TLS), sind Filter auf der Anwendungsschicht nicht mehr in der Lage, die Nutzdaten z. B. in Hinblick auf Viren oder andere Schadprogramme zu kontrollieren. Auch die Protokollierungsmöglichkeiten werden durch eine Verschlüsselung stark eingeschränkt. Eine erste ad-hoc-Lösung könnte darin bestehen, nur von bestimmten internen Rechnern den Aufbau von TLS-Verbindungen zu erlauben, u.U. nur zu ausgewählten Zielsystemen. Andererseits sind die Daten selbst dann geschützt, wenn AngreiferInnen das Application-Gateway unter ihre Kontrolle gebracht haben.

Eine temporäre Entschlüsselung auf einer Filterkomponente zu Analysezwecken ist weder praktikabel noch wünschenswert.

Eine generelle Empfehlung für oder gegen den Einsatz von Verschlüsselung über oder an der Firewall kann nicht gegeben werden, dies hängt von den Anforderungen im Einzelfall ab.

13.1.18 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Kommunikationsnetze transportieren Daten zwischen IT-Systemen. Dabei werden die Daten selten über eine dedizierte Kommunikationsleitung zwischen den an der Kommunikation beteiligten Partnern übertragen. Vielmehr werden die Daten über viele Zwischenstationen geleitet. Je nach Kommunikationsmedium und verwendeter Technik können die Daten von den Zwischenstationen unberechtigt abgehört werden, oder auch von im jeweiligen Vermittlungsnetz angesiedelten Dritten (z. B. bei der Verwendung des Ethernetprotokolls ohne Punkt-zu-Punkt-Vernetzung). Da die zu übertragenden Daten nicht von unberechtigten Dritten abgehört, verändert oder zur späteren Wiedereinspeisung in das Netz (Replay-Attacke) benutzt werden sollen, muss ein geeigneter Mechanismus eingesetzt werden, der dies verhindert. Verschlüsselung der Daten mit - wenn nötig - gegenseitiger Authentifizierung der Kommunikationspartner kann diese Gefahr (je nach Stärke des gewählten Verschlüsselungsverfahrens sowie der Sicherheit der verwendeten Schlüssel) reduzieren.

In der Regel kommunizieren Anwendungen miteinander, um anwendungsbezogene Informationen auszutauschen. Die Verschlüsselung der Daten kann nun auf mehreren Ebenen erfolgen:

- Auf Applikationsebene:
  Die kommunizierenden Applikationen müssen dabei jeweils über die entsprechenden Ver- und Entschlüsselungsmechanismen verfügen.
- Auf Betriebssystemebene:
  Die Verschlüsselung wird vom lokalen Betriebssystem durchgeführt. Jegliche Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt.
- Auf Netzkoppelelementebene:
  Die Verschlüsselung findet zwischen den Netzkoppelelementen (z. B. Router) statt.

Die einzelnen Mechanismen besitzen spezifische Vor- und Nachteile. Die Verschlüsselung auf Applikationsebene hat den Vorteil, dass die Verschlüsselung vollständig der Kontrolle der jeweiligen Applikation unterliegt. Ein Nachteil ist, dass zur verschlüsselten Kommunikation nur eine mit demselben Verschlüsselungsmechanismus ausgestattete Partnerapplikation in Frage kommt. Weiters können entsprechende Authentifizierungsmechanismen zwischen den beiden Partnerapplikationen zur Anwendung kommen.

Im Gegensatz dazu findet die Verschlüsselung im Fall der Verschlüsselung auf Betriebssystemebene transparent für jede Applikation statt. Jede Applikation kann mit jeder anderen Applikation verschlüsselt kommunizieren, sofern das Betriebssystem, unter dem die Partnerapplikation abläuft, über den Verschlüsselungsmechanismus verfügt. Nachteilig wirkt sich hier aus, dass bei einer Authentifizierung lediglich die Rechner gegenseitig authentifiziert werden können, und nicht die jeweiligen Partnerapplikationen.

Der Einsatz von verschlüsselnden Netzkoppelelementen besitzt den Vorteil, dass applikations- und rechnerseitig keine Verschlüsselungsmechanismen vorhanden sein müssen. Die Verschlüsselung ist auch hier transparent für die Kommunikationspartner, allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und birgt damit ein Restrisiko. Authentifizierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden hier nicht authentifiziert.

Werden sensitive Daten über ein Netz (auch innerhalb des Intranets) übertragen, empfiehlt sich der Einsatz von Verschlüsselungsmechanismen. Bieten die eingesetzten Applikationen keinen eigenen Verschlüsselungsmechanismus an oder wird das angebotene Verfahren als zu schwach eingestuft, so sollte von der Möglichkeit der betriebssystemseitigen Verschlüsselung Gebrauch gemacht werden. Hier bieten sich z. B. Verfahren wie TLS an, die zur transparenten Verschlüsselung auf Betriebssystemebene entworfen wurden. Je nach Sicherheitspolitik können auch verschlüsselnde Netzkoppelelemente eingesetzt werden, etwa um ein virtuelles privates Netz (VPN) mit einem Kommunikationspartner über das Internet zu realisieren. Entsprechende Softwaremechanismen sind in der Regel auch in Firewall-Systemen verfügbar.

Erfolgt der Zugang auf sensible Daten über einen externen Zugang, so sind kryptographische Einmalverfahren mit einer Besitzkomponente einzusetzen. Wegen der einheitlichen Administrierbarkeit wird empfohlen für den Zugang die Bürgerkarte/ Dienstkarte und MOA-ID zu verwenden [IKTB-140605-01] .

Beim Einsatz von verschlüsselter Kommunikation und gegenseitiger Authentifizierung sind umfangreiche Planungen im Rahmen der Sicherheitspolitik eines Unternehmens bzw. einer Behörde nötig. Im Rahmen der hier angesprochenen Kommunikationsverschlüsselungen sind insbesondere folgende Punkte zu beachten:

- Welche Verfahren sollen zur Verschlüsselung benutzt werden bzw. werden angeboten (z. B. in Routern)?
- Unterstützen/Nutzen die eingesetzten Verschlüsselungsmechanismen existierende oder geplante Standards (IPsec, IPv6, IKE; TLS); vgl. dazu auch 13.2.3.5 Geeignete Auswahl eines E-Mail-Clients/-Servers zu Zugang zu E-Mail.
- Sind gemäß der Sicherheitspolitik ausreichend starke Verfahren und entsprechend lange Schlüssel gewählt worden?
- Werden die Schlüssel sicher aufbewahrt?
- Werden die Schlüssel in einer sicheren Umgebung erzeugt, und gelangen sie auf sicherem Weg zum notwendigen Einsatzpunkt (Rechner, Softwarekomponente)?
- Sind Schlüssel-Recovery-Mechanismen nötig?

Ähnliche Fragestellungen sind bei der Nutzung von Zertifikaten zur Authentifizierung von Kommunikationspartnern zu beachten.

Im Bereich der öffentlichen Verwaltung sind außerdem bezüglich der Verschlüsselung des E-Mail-Verkehrs entsprechende Vorgaben, wie etwa die Vorgabe der Eigenschaften von Verschlüsselungszertifikaten gemäß des IKT-Board-Beschlusses [IKTB-181202-1] zu beachten.

13.2 Informations- und Datenaustausch

Der elektronische Austausch von Informationen und Daten bedarf der Entwicklung geeigneter Richtlinien und der Anwendung sicherer Verfahren zum Schutz der ausgetauschten Informationen und der dabei verwendeten Datenübertragungstechnologien. Dies betrifft sowohl den Informationsaustausch innerhalb der Organisation als auch den Austausch von Informationen mit externen Entitäten über die eigenen Organisationsgrenzen hinaus. Etwaige Austauschvereinbarungen mit den involvierten Kommunikationspartnern und die aktuell geltenden einschlägigen Gesetze sind dabei jederzeit einzuhalten.

13.2.1 Richtlinien beim Datenaustausch mit Dritten

Beim regelmäßigen Datenaustausch mit Dritten ist die Festlegung von Richtlinien bzw. der Abschluss von Vereinbarungen mit allen Beteiligten sinnvoll. Dabei spielt es keine Rolle, wie der Datenaustausch selbst erfolgt (z.B. Datenträgeraustausch, E-Mail, etc.).

In einer derartigen Vereinbarung können Angaben zu folgenden Aspekten enthalten sein:

- Bestimmung der Verantwortlichen,
- Benennung von Ansprechpartnern (in technischen, organisatorischen und sicherheitstechnischen Belangen),
- Notwendigkeit eines Non-Disclosure-Agreements (NDA),
- Einstufung von Übertragungsverfahren für klassifizierte Informationen nach [InfoSiG],
- Festlegung der Datennutzung,
- Definition von Anwendungen und Datenformaten,
- Festlegung technischer Übertragungskanäle,
- Definition von Programmen zum Schutz der Daten,
- Festlegung technischer Mittel zur Prüfung der Datenintegrität,
- Definition von Details zu Überprüfungen auf Schadsoftware,
- Festlegung von Fristen zur Datenlöschung,
- Regelung des Managements kryptographischer Schlüssel und Zertifikate, falls erforderlich,

- Einhaltung einschlägiger Gesetze (bspw. Datenschutzgesetz, etc.) und
- Umgang mit Pflichten, die sich aus relevanten Gesetzen (z.B. Datenschutz-Folgenabschätzung) ergeben.

Weitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in 8.3.2 Datenträgerverwaltung und 8.3.3 Datenträgeraustausch.

13.2.2 Vertraulichkeitsvereinbarungen

Externe MitarbeiterInnen oder Subunternehmen benötigen und erhalten häufig für die Erfüllung ihrer Aufgaben Zugang zu vertraulichen bzw. klassifizierten Informationen nach dem [InfoSiG] oder erzielen Ergebnisse, die vertraulich behandelt werden müssen. In diesen Fällen müssen sie rechtlich bindend verpflichtet werden, diese entsprechend zu behandeln. Hierüber sind Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements - NDAs) abzuschließen, die von den externen MitarbeiterInnen unterzeichnet werden.

Eine Vertraulichkeitsvereinbarung bietet die rechtliche Grundlage für die Verpflichtung externer MitarbeiterInnen zur vertraulichen Behandlung von Informationen. Aus diesem Grund muss sie den geltenden Gesetzen und Bestimmungen für die Organisation in dem speziellen Einsatzbereich entsprechen und diese berücksichtigen. Sie muss klar formuliert sein und stets aktuell gehalten werden. Ebenso kann ein NDA, das beispielsweise auch ohne gegenseitige Unterschrift der Vertragsparteien gültig ist, öffentlich abrufbar sein (z.B. über die Webseite). Dann aber sollte darauf geachtet werden, dass keine persönlichen oder vertraulichen Daten darin enthalten sind.

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein:

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt bzw. ob die Vertraulichkeit für einen unbeschränkten Zeitraum sicherzustellen ist,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Löschung bzw. Vernichtung oder Rückgabe von Daten bzw. Datenträgern,
- wie die Eigentumsrechte an Informationen resp. geistigem Eigentum geregelt sind,
- welche Verwendung der Informationen zulässig ist,
- allfällige Kontrollrechte des Urhebers bzw. der überlassenden Organisation,
- allfällige Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner, etwa Pflicht zur Überbindung der Vertraulichkeitsvereinbarung,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten, etwa Strafzahlungen bzw. Haftungen und
- in welche Gerichtsbarkeit die Vertraulichkeitsvereinbarung fällt.

In der Vertraulichkeitsvereinbarung kann auch auf die relevanten Sicherheitsrichtlinien und weitere Richtlinien der Organisation hingewiesen werden. In dem Fall, dass externe MitarbeiterInnen Zugang zur organisationsinternen IT-Infrastruktur erhalten, sollten diese neben der Vertraulichkeitsvereinbarung auch die IT-Sicherheitsrichtlinien für die Nutzung der jeweiligen IT-Systeme unterzeichnen.

Es kann sinnvoll sein, verschiedene Vertraulichkeitsvereinbarungen - je nach Einsatzzweck - zu verwenden. In diesem Fall muss klar definiert werden, welche Vereinbarungen für welche Fälle notwendig sind.

Diesbezügliche Mustervorlagen sind unter B.5 angeführt.

[Quelle: BSI M 3.55]

13.2.3 E-Mail

Trotz diverser bekannter Limitierungen in Bezug auf Funktionalität und Sicherheit ist E-Mail nach wie vor eine der dominierenden Technologien für den elektronischen Austausch von Daten und Informationen, sowohl im privaten als auch im beruflichen Umfeld. Aufgrund dieser gegebenen praktischen Relevanz wird IT-Sicherheit im Kontext der Verwendung von E-Mail als Kommunikationstechnologie an dieser Stelle im Detail betrachtet. Dies ist vor allem deswegen notwendig, weil E-Mail ursprünglich nicht für einen sicheren Datenaustausch konzipiert wurde und die Technologie daher einige inhärente Schwachstellen aufweist, denen sich BenutzerInnen bewusst sein müssen bzw. denen durch geeignete Maßnahmen begegnet werden muss. Relevante Sicherheitsaspekte in Bezug auf die Verwendung von E-Mail werden in den folgenden Unterabschnitten diskutiert.

13.2.3.1 Festlegung einer Sicherheitspolitik für E-Mail-Nutzung

Bevor ein Einsatz von E-Mail als Kommunikationstechnologie in Betracht gezogen wird, sollte festgelegt werden, für welche Anwendungsfälle eine Verwendung von E-Mail überhaupt vorgesehen werden kann. Diese Entscheidung muss unter anderem abhängig gemacht werden vom Schutzbedarf der zu übermittelnden Informationen und Daten. Zur Eruierung des Schutzbedarfs müssen zumindest deren Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität berücksichtig werden. Im Allgemeinen sollte E-Mail – insbesondere ohne zusätzliche Schutzfunktionen – nur zur Übertragung unkritischer oder wenig kritischer Informationen und Daten verwendet werden.

Wird in einer Organisation die Entscheidung getroffen, bisher händisch bearbeitete Geschäftsprozesse ab sofort per E-Mail durchzuführen, muss vorab geklärt werden, wie Anmerkungen an Vorgängen wie Verfügungen, Abzeichnungen oder Schlusszeichnungen, die bisher handschriftlich angebracht wurden, elektronisch abgebildet werden können.

Weiters ist festzulegen, ob und in welchem Rahmen eine private Nutzung der E-Mail-Infrastruktur der Organisation erlaubt ist. Das ist insbesondere dann relevant, wenn Bring-Your-Own-Device-Konzepte (BYOD) umgesetzt sind. Darüber hinaus ist eine solche Regelung auch dann von besonderer Bedeutung, wenn Home-Office Bestandteil des Organisationskonzepts ist.

Die Organisation muss zudem eine E-Mail-Sicherheitspolitik festlegen, in der unter anderem folgende Punkte beschrieben und geregelt sind:

- Wer einen Zugang zur E-Mail-Infrastruktur der Organisation erhält,
- welche Regelungen von den E-Mail-AdministratorInnen und den E-Mail-BenutzerInnen zu beachten sind (vgl. 13.2.3.2 Regelung für den Einsatz von E-Mail),
- bis zu welchem Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Authentizität Informationen per E-Mail versandt werden dürfen,
- ob und unter welchen Rahmenbedingungen eine private Nutzung der E-Mail-Infrastruktur der Organisation erlaubt ist,
- wie die BenutzerInnen hinsichtlich Funktion und Sicherheit geschult werden und
- wie jederzeit technische Hilfestellung für die BenutzerInnen gewährleistet wird.

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zu gewährleisten:

- Für Organisationen im öffentlichen Bereich sind vorhandene einschlägige Richtlinien zu berücksichtigen (z.B. Konventionen unter [IKT-KON]).
- Geschützte E-Mail-Kommunikation setzt eine sichere Basis-Architektur (z.B.: sichere E-Mail-Server, sichere E-Mail-Clients, geschützte Anbindung der Clients an die Server, Verwendung von kryptographischen Verfahren) voraus.
- Die E-Mail-Programme der BenutzerInnen müssen durch die Systemadministration so vorkonfiguriert sein, dass ohne weiteres Zutun der BenutzerInnen maximale Sicherheit erreicht werden kann (siehe auch 13.2.3.6 Sichere Konfiguration der E-Mail-Clients).
- Für E-Mail-Adressen sind Namenskonventionen festzulegen. Insbesondere ist darauf zu achten, dass Sonderzeichen (Umlaute, …) vermieden werden, da diese Kodierungsprobleme und damit Funktionsbeeinträchtigungen verursachen können.
- Neben personenbezogenen E-Mail-Adressen können auch organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden. Dies ist insbesondere bei zentralen Anlaufstellen wichtig.

- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung, Authentisierung und Prüfung der Berechtigungen des Senders beim Übertragungssystem möglich sein.
- Die BenutzerInnen müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zur Dateiübermittlung müssen ihnen bekannt sein.
- Zur Beschreibung des Absenders werden bei E-Mails üblicherweise so genannte Signaturen (Absenderangaben, nicht zu verwechseln mit kryptographischen elektronischen/digitalen Signaturen) an das Ende der E-Mail angefügt.
  Der Inhalt einer Signatur sollte dem eines Briefkopfs ähneln, also Name, Organisationsbezeichnung und Kontaktdaten enthalten. Gleichzeitig sollte eine Signatur aus Gründen der Übersichtlichkeit nicht zu umfangreich sein.
  Die Behörde bzw. das Unternehmen sollte einen Standard für die einheitliche Gestaltung von Signaturen festlegen.
- Von den eingesetzten Sicherheitsmechanismen hängt es ab, bis zu welchem Schutzbedarf (z.B.: normal, hoch) Daten per E-Mail versandt werden dürfen. Es ist grundsätzlich festzulegen, ob E-Mails bzw. Attachments in verschlüsselter Form übertragen werden dürfen. Dies erhöht zwar die Sicherheit gegen unautorisiertes Lesen oder Verändern von Inhalten, erschwert aber die Suche nach Schadsoftware oder macht sie gänzlich unmöglich. Es ist denkbar, dass E-Mails in denen verschlüsselte Dateien enthalten sind von Firewalls auf der Empfängerseite blockiert werden und den Empfänger bzw. die Empfängerin nie erreichen. Ist der Einsatz von Verschlüsselungsverfahren prinzipiell erlaubt, so sollte geregelt werden, ob und wann übertragene Dateien verschlüsselt werden müssen (siehe auch 10.1 Einsatz kryptographischer Maßnahmen).
  Gleichermaßen ist festzulegen, ob und in welcher Form kryptographische Mechanismen zur Überprüfung der Integrität von Daten (z.B. über MACs - Message Authentication Code, digitale/elektronische Signaturen, …) eingesetzt werden dürfen bzw. müssen. Es ist zentral festzulegen, welche Applikationen für die Verschlüsselung bzw. den Einsatz von elektronischen Signaturen von BenutzerInnen zu verwenden sind. BenutzerInnen müssen diese Anwendungen zur Verfügung gestellt bekommen und in deren Anwendung unterwiesen werden. Für die Verwaltung notwendiger kryptographischer Schlüssel und Zertifikate sollte ein geeignetes Schlüssel- und Zertifikat-Management in der Organisation etabliert werden.
- Es sollte festgelegt werden, unter welchen Bedingungen ein- oder ausgehende E-Mails zusätzlich ausgedruckt werden müssen. Aus Gründen des Umweltschutzes und der Sicherheit sollte das Ausdrucken von E-Mails auf das absolut notwendige Minimum reduziert werden.
- Die Dateiübertragung kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Bei der Übertragung personenbezogener Daten sind die gesetzlichen Vorgaben zur Protokollierung zu beachten.

- Ob und wie ein externer Zugang zu E-Mail-Diensten der Organisation technisch und organisatorisch realisiert werden soll, ist zu prüfen und muss festgelegt werden. Technisch ist ein E-Mail-Zugang insbesondere außerhalb des organisationsinternen Netzwerks geeignet abzusichern, z. B. über VPN.

E-Mails, die intern versendet werden, dürfen das interne Netz nicht verlassen. Dies ist durch die entsprechenden technisch-administrativen Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das ungesicherte Internet erfolgen. Durch Anwendung geeigneter Techniken, wie z. B. VPN, entfällt diese Forderung, wenn Nachrichten entsprechend verschlüsselt werden.

13.2.3.2 Regelung für den Einsatz von E-Mail

Beim Einsatz von E-Mail in der Organisation sind u. a. folgende Punkte zu beachten:

- Die Adressierung von E-Mails muss korrekt erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Innerhalb einer Organisation sollten daher Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Durch den Versand von Testnachrichten an neue E-Mail-Adressen ist die korrekte Zustellung von Nachrichten zu prüfen.
- Für alle nach außen gehenden E-Mails sollte eine Signatur (Absenderangabe am Ende der E-Mail) verwendet werden.
- Ausgehende E-Mails sollten protokolliert werden, da bei E-Mails nicht automatisch von einer erfolgreichen Zustellung ausgegangen werden kann, E-Mails also auch verloren gehen können.
- Die Betreffangabe (Subject) der E-Mail sollte immer ausgefüllt werden, z. B. entsprechend der Betreffangabe in einem handschriftlichen Anschreiben.
- Die Korrektheit der durchgeführten Datenübertragung sollte überprüft werden, da bei der Verwendung von E-Mail ohne zusätzliche kryptographische Sicherheitsmaßnahmen nicht davon ausgegangen werden kann, dass Daten während des Transports unverändert bleiben.
- Vor dem Absenden bzw. vor der Dateiübermittlung sind die ausgehenden Dateien über die Verwendung geeigneter Virenscanner explizit auf Schadsoftware zu überprüfen.
- Erfolgt über die E-Mail auch eine Dateiübertragung, so sollten die folgenden Informationen an die EmpfängerInnen zusätzlich übermittelt werden:
    - Art der Datei (z. B. MS Word),
    - Kurzbeschreibung über den Inhalt der Datei,
    - Hinweis, dass Dateien auf Schadsoftware überprüft sind,
    - ggf. Art des verwendeten Packprogramms (z. B. 7-ZIP)

    - ggf. Art der eingesetzten Software für Verschlüsselung bzw. elektronische Signatur.

  Jedoch sollte nicht vermerkt werden:

    - welches Passwort für die eventuell geschützten Informationen vergeben wurde,
    - welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde.
- Regelmäßiges Löschen von E-Mails: E-Mails sollten nicht unnötig lange im Posteingang gespeichert werden. Sie sollten entweder nach dem Lesen gelöscht werden oder in Benutzerverzeichnissen gespeichert werden, wenn sie erhalten bleiben sollen. Viele E-Mail-Programme löschen E-Mails nicht sofort, sondern transferieren sie in spezielle Ordner. BenutzerInnen müssen darauf hingewiesen werden, wie sie E-Mails (sowohl auf ihren Clients als auch am Server) vollständig löschen können.

Bei E-Mail-Systemen werden Informationen potenziell unverschlüsselt über offene bzw. ungeschützte Leitungen transportiert und demzufolge unter Umständen auf diversen Zwischenrechnern gespeichert, bis sie schließlich ihre EmpfängerInnen erreichen. Auf dem Übertragungsweg können ungeschützte Informationen daher leicht manipuliert und/oder eingesehen werden. Aber auch die VersenderInnen einer E-Mail haben meist die Möglichkeit, ihre Absenderadresse (From) beliebig einzutragen, so dass grundsätzlich nicht von einer Echtheit der Absenderangabe ausgegangen werden kann und die Authentizität des Absenders nur über Rückfrage oder durch Benutzung von digitalen Signaturen sichergestellt werden kann. Darüber hinaus wird selbst bei elektronisch signierten E-Mails der Betreff nicht signiert, wodurch auch dieser Betreff auf dem Übertragungsweg manipuliert werden kann. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage (z.B. telefonisch) oder durch den Einsatz von digitalen Signaturen (vgl. 10.1 Einsatz kryptographischer Maßnahmen) überprüft werden.

Bei Verwendung von Verschlüsselung ist zu beachten, dass verschlüsselte Nachrichten i. Allg. nicht zentral auf Schadsoftware überprüft werden können (dazu wäre eine Entschlüsselung und damit die zentrale Hinterlegung der dafür notwendigen Schlüssel erforderlich). Es ist daher in der E-Mail-Sicherheitspolitik festzulegen, ob verschlüsselte Nachrichten zugelassen sind und wie damit zu verfahren ist. Wenn verschlüsselte Nachrichten nicht zugelassen sind, können diese etwa durch einen Postmaster (siehe 13.2.3.4 Einrichtung eines Postmasters) blockiert werden.

Es ist festzulegen, ob und gegebenenfalls in welchem Rahmen eine private Nutzung von E-Mail-Diensten der Organisation zulässig ist. Diese Festlegung sollte im Rahmen einer Betriebsvereinbarung oder bei Abschluss des Arbeitsvertrages getroffen werden. Weiters sind auch die zulässigen Kontrollmaßnahmen des Arbeitgebers/der Arbeitgeberin (Protokollierung, Auswertung, …) und die möglichen Sanktionen bei Verstößen gegen die getroffenen Vereinbarungen zu regeln.

Alle Regelungen und Bedienungshinweise zum Einsatz von E-Mail sind schriftlich zu fixieren und sollten den MitarbeiterInnen jederzeit zur Verfügung stehen.

Die BenutzerInnen müssen vor dem Einsatz in Bezug auf die Verwendung von E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mails sensibilisiert werden. Besonderes Augenmerk ist hierbei auf Gefahren, die sich durch Phishing-E-Mails ergeben, zu legen.

Zur Vermeidung des Missbrauchs von E-Mail-Infrastrukturen sind die MitarbeiterInnen über potenzielles Fehlverhalten zu belehren. Sie sollten dabei unter anderem vor der Teilnahme an E-Mail-Kettenbriefen, vor Spams, der unnötigen Weiterverbreitung von Viruswarnungen sowie vor dem Abonnement umfangreicher Mailinglisten gewarnt werden.

BenutzerInnen müssen darüber informiert werden, dass Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch auf Informationsservern eingestellt noch nachgefragt werden dürfen.

Außerdem sollten BenutzerInnen dazu verpflichtet werden, dass bei der Nutzung von Kommunikationsdiensten

- die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muss (vgl. dazu § 126a Datenbeschädigung (StGB)). Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erhalten, Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung einer Netznutzerin bzw. eines Netznutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben,
- die Verbreitung von für die Allgemeinheit irrelevanten Informationen unterlassen werden muss,
- Eindringversuche an internen/externen Netzen/Geräten zu unterlassen sind und
- die Verbreitung von redundanten Informationen vermieden werden sollte.

13.2.3.3 Sicherer Betrieb eines E-Mail-Servers

Der sichere Betrieb eines E-Mail-Servers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der E-Mail-Server nimmt von anderen E-Mail-Servern E-Mails entgegen und leitet sie an die angeschlossenen BenutzerInnen oder E-Mail-Server weiter. Weiters reicht der E-Mail-Server die gesendeten E-Mails lokaler BenutzerInnen an externe E-Mail-Server weiter. Der E-Mail-Server muss hierbei sicherstellen, dass lokale E-Mails der angeschlossenen BenutzerInnen nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können.

Die E-Mails werden vom E-Mail-Server bis zur Weitergabe zwischengespeichert. Viele Internetprovider und AdministratorInnen archivieren zusätzlich die ein- und ausgehenden E-Mails. Damit Unbefugte nicht über den E-Mail-Server auf Nachrichteninhalte zugreifen können, muss der E-Mail-Server gegen unbefugten Zugriff gesichert sein (vgl. dazu § 126a Datenbeschädigung (StGB)). Dafür sollte er gesichert (in einem Serverraum oder Serverschrank) aufgestellt sein. Für den ordnungsgemäßen Betrieb sind AdministratorInnen und StellvertreterInnen zu benennen und für den Betrieb des E-Mail-Servers und des zugrunde liegenden Betriebssystems zu schulen. Es muss ein Postmaster-Account eingerichtet werden, an den alle unzustellbaren E-Mails und alle Fehlermeldungen weitergeleitet werden (siehe auch 13.2.3.4 Einrichtung eines Postmasters).

Auf die E-Mail-Boxen der lokal angeschlossenen BenutzerInnen dürfen nur diese Zugriff haben. Auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden (z. B. Spooldateien), ist der Zugriff auch für die lokalen BenutzerInnen zu unterbinden.

Im laufenden Betrieb muss regelmäßig kontrolliert werden, ob die Verbindung mit den benachbarten E-Mail-Servern, insbesondere dem E-Mail-Server des E-Mail-Providers, noch stabil ist. Außerdem muss im Betreib sichergestellt sein, dass der für die Zwischenspeicherung der E-Mails zur Verfügung stehende Speicherplatz noch ausreicht, da ansonsten kein weiterer Nachrichtenaustausch möglich ist.

Umfang und Inhalt der Protokollierung der Aktivitäten des E-Mail-Servers sind vorab festzulegen.

Der E-Mail-Server sollte ein abgeschlossenes, eigenes Produktionssystem sein, insbesondere sollten von der Verfügbarkeit des E-Mail-Servers keine weiteren Dienste abhängig sein. Es sollte jederzeit kurzfristig möglich sein, ihn abzuschalten, z. B. bei Verdacht auf Kompromittierung.

Die Benutzernamen auf dem E-Mail-Server sollten nicht aus den E-Mail-Adressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzeraccounts zu erschweren.

Eingehende E-Mails sollten auf der Firewall oder am E-Mail-Server auf Schadsoftware überprüft werden (vgl. auch 13.1.16 Firewalls und aktive Inhalte).

Über Filterregeln können für bestimmte E-Mail-Adressen der Empfang oder die Weiterleitung von E-Mails gesperrt werden. Dies kann z. B. sinnvoll sein, um sich vor Spam-Mail zu schützen (sogenanntes negatives Sicherheitsmodell, auch „Blacklisting“). Auch über die Filterung anderer Header-Einträge kann versucht werden, Spam auszugrenzen. Hierbei muss mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen. Daher sollten entsprechende Filterregeln sehr genau definiert werden, indem beispielsweise aus jeder Spam-Mail eine neue dedizierte Filterregel abgeleitet wird.

Es ist festzulegen, welche Protokolle und Dienste am E-Mail-Server erlaubt sind.

Ein E-Mail-Server sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte ein E-Mail-Server so konfiguriert werden, dass er E-Mails nur für die Organisation selbst entgegennimmt und nur E-Mails verschickt, die von MitarbeiterInnen der Organisation stammen.

Wenn eine Organisation keinen eigenen E-Mail-Server betreibt, sondern über einen oder mehrere E-Mail-Clients direkt auf den E-Mail-Server eines externen Providers (z.B. Anbieter eines Cloud-Service, der E-Mail in Form eines SaaS-Dienstes anbietet) zugreift, muss mit diesem Provider ein entsprechender Vertrag abgeschlossen werden. Dieser muss neben funktions- und verfügbarkeitsbezogenen Vereinbarungen unter anderem auch relevante datenschutzrechtliche Aspekte beinhalten und regeln (z.B. gemäß Art. 28 EU-DSGVO).

13.2.3.4 Einrichtung eines Postmasters

> *In größeren Organisationen sollte zum reibungslosen Betrieb des E-Mail-Dienstes ein „Postmaster“ benannt werden.*

Dieser nimmt folgende Aufgaben wahr:

- Bereitstellen der E-Mail-Dienste auf lokaler Ebene,
- Pflege der Adresstabellen,
- Überprüfung, ob die externen Kommunikationsverbindungen funktionieren,
- Etablierung technischer Maßnahmen zur automatisierten Überprüfung von Attachments auf Schadsoftware,
- Setzen technischer und organisatorischer Maßnahmen zum Umgang mit gefundener Schadsoftware (Verhinderung einer Weiterleitung, Ablage in speziellen Quarantänebereichen, Verständigung der betroffenen Benutzer, …),
- Implementierung von technischen Maßnahmen zur automatisierten Überprüfung der Compliance von E-Mail-Inhalten in Bezug auf gültige Dokumentformate,

- Setzen von Maßnahmen, wenn der Inhalt einer E-Mail (zur Gänze oder teilweise) nicht einem gültigen Dokumentenaustauschformat entspricht (etwa Blocken der Nachricht, Verständigung des Absenders/der Absenderin bzw. des Empfängers/der Empfängerin, Speicherung in einem Zwischenbereich, automatische Löschung nach einer vorgegebenen Zeitspanne, evtl. Freigabe durch Sicherheitsbeauftragte nach Rücksprache und Begründung),
- Anlaufstelle bei E-Mail-Problemen für EndbenutzerInnen sowie für die Betreiber von Gateway- und Relaydiensten.

Prinzipiell müssen alle unzustellbaren E-Mails und alle Fehlermeldungen an den Postmaster weitergeleitet werden, der versuchen sollte, die Fehlerquellen zu beheben. E-Mails, die unzustellbar bleiben, müssen nach Ablauf einer vordefinierten Frist vernichtet werden, die AbsenderInnen (besser: die zustellenden Server) sind mittels einer entsprechenden Fehlermeldung zu informieren.

Zuständige BetreuerInnen (evtl. Hotline oder Helpdesk) sollten jederzeit von BenutzerInnen telefonisch erreicht werden können.

13.2.3.5 Geeignete Auswahl eines E-Mail-Clients/-Servers

Softwarekomponenten, die für den Betrieb und die Verwendung der E-Mail-Infrastruktur notwendig sind (z.B. E-Mail-Clients und E-Mail-Server), sollten unter dem Gesichtspunkt offener internationaler Standards gewählt werden.

Unter anderem sollte auf die Einhaltung folgender Mindesteigenschaften geachtet werden:

- Kommunikation:
  Für die Kommunikation zwischen Clients und Servern im E-Mail-Verkehr sowie für die Kommunikation zwischen E-Mail-Servern selbst sollten etablierte Protokolle wie POP3 [RFC 1939], IMAP4 [RFC 3501], Exchange oder SMTP [RFC 5321] verwendet werden.
- Adress-Verwaltung:
  Die Verwaltung von E-Mail-Adressen und Attributen erfolgt in Verzeichnisdiensten. Eine komfortable Umsetzung erfordert, dass die eingesetzten Clients und Server entsprechende Interfaces zu diesen Verzeichnisdiensten aufweisen. Dafür eignet sich der Standard LDAP V3 [RFC 4511].
- Sicherheit:
  Für die E-Mail-Sicherheit ist S/MIME V4 einzusetzen. Die Verschlüsselungen und Signaturen müssen jedenfalls kompatibel zu CMS (Cryptographic Message Syntax) sein. In Bezug auf die eingesetzten Schlüssellängen der symmetrischen Schlüsselkomponenten müssen einschlägige Vorgaben und Empfehlungen

berücksichtigt werden (siehe z.B. Sicherheitsempfehlungen für Behörden - A-SIT). Für die Signatur von Attachments sind als Signaturformate PKCS#7 oder XML zu verwenden. PGP kann für die Vertraulichkeit in einer Übergangszeit in manchen Bereichen notwendig bleiben.

- Zugang von außen:
  Der uneingeschränkte Zugang von außen ist nur über eine geeignete Verschlüsselung einzurichten (z. B. VPN mit oder ohne IPsec), die auch die eine Ende-zu-Ende-Authentifizierung sicherstellt. E-Mail-Zugänge über Web-Interfaces müssen zumindest verschlüsselt sein (Standard TLS oder IPsec mit einer geeigneten symmetrischen Schlüssellänge (siehe z.B. Sicherheitsempfehlungen für Behörden - A-SIT)). Darüber hinaus gilt es, die existierende Webmail-Policy (sowie vorhandene Checklisten) zu beachten.
- Nachweis der Standardkonformität:
  Für die Bereiche der öffentlichen Verwaltung wird ein Testmailservice angeboten. Dieses dient zur Kompatibilitätsfeststellung der eingesetzten Systeme sowohl nach innen als auch nach außen. Damit kann der Nachweis der Konformität der Systeme mit den geforderten Standards und der Einhaltung der Mindestantwortzeiten erbracht werden.

13.2.3.6 Sichere Konfiguration der E-Mail-Clients

Die E-Mail-Programme der BenutzerInnen müssen durch die AdministratorInnen so vorkonfiguriert sein, dass ohne weiteres Zutun der BenutzerInnen maximale Sicherheit erreicht werden kann. Die BenutzerInnen sind darauf hinzuweisen, dass sie die Konfiguration nicht selbsttätig ändern dürfen, bzw. sollten BenutzerInnen wenn möglich technisch gar nicht die Möglichkeit eingeräumt bekommen, Konfigurationen zu ändern.

Insbesondere sollten bei der Konfiguration der E-Mail-Clients folgende Punkte berücksichtigt werden:

- Das E-Mail-Passwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Passwort auf der Client-Festplatte abgelegt, u.U. sogar im Klartext oder nur schwach verschlüsselt. Jede/r, die/der Zugriff auf den E-Mail-Client hat, hat so die Möglichkeit, unter fremdem Namen E-Mails zu verschicken bzw. das E-Mail-Passwort auszulesen.
- Als Reply-Adresse ist die E-Mail-Adresse der BenutzerInnen einzustellen, um sicherzustellen, dass keine internen E-Mail-Adressen weitergegeben werden.

Bei der Konfiguration von E-Mail-Clients kann auf produktbezogene und aktuelle von vertrauenswürdigen Stellen veröffentlichte Leitlinien zurückgegriffen werden.

13.2.3.7 Verwendung von „Webmail“ externer Anbieter

Eine Vielzahl von externen E-Mail-Diensteanbietern stellen ihre Services oft kostenlos (evtl. in Verbindung mit Werbung) zur Verfügung. In diesem Zusammenhang wird der Zugang zu den E-Mail-Konten in der Regel via „Webmail“ angeboten, indem die AnwenderInnen die E-Mail-Dienste ohne jegliche clientseitige E-Mail-Software sondern nur unter Verwendung des Browsers nutzen können.

Die Anbieter derartiger Webmail-Dienste unterscheiden sich nicht nur hinsichtlich ggf. anfallender Kosten, es ergeben sich auch Unterschiede bezüglich E-Mail-Box-Größen, Verfügbarkeit, dem Einsatz von Spam-Filtern usw. Vor allem aus Datenschutzgründen relevant kann auch der Ort sein, an dem Anbieter anfallende E-Mail-Daten speichern. Diesbezüglich ist eine genaue Durchsicht der Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Anbieters vorzunehmen. Darüber hinaus sind die gebotenen Sicherheitsaspekte zu beachten, wie etwa:

- Ist es möglich, über eine verschlüsselte Verbindung (z. B. TLS) auf die eigene E-Mail-Box zuzugreifen?
- Können E-Mails elektronisch signiert und verschlüsselt werden?
- Findet eine zuverlässige Identitätsprüfung von Neukunden statt?
- Wird der Service durch fachkundiges und sicherheitstechnisch geschultes Personal realisiert und betrieben (Social Engineering Attacken: beispielsweise soll das Erfragen des Passwortes durch einen fingierten Anruf am Helpdesk nicht möglich sein)?
- Eine Prüfung der E-Mails auf Schadsoftware sollte anbieterseitig gewährleistet sein.
- Spam-Filter sollten zur Verfügung stehen.

Bei der Verwendung von Webmail sollten die AnwenderInnen Folgendes beachten (vgl. auch 13.2.3.5 Geeignete Auswahl eines E-Mail-Clients/-Servers):

- Wahl eines geeigneten Passwortes (vgl. 9.3.1 Regelungen des Passwortgebrauches).
- Wenn möglich, die Mehrfaktorauthentifizierung aktivieren.
- Zugriffe auf das Webmail-Konto dürfen nur über verschlüsselte Verbindungen auf der Grundlage aktueller Versionen erfolgen (z.B. TLS und zusätzlich im Idealfall über eine VPN-Verbindung).
- Trotz eines vorhandenen anbieterseitigen Schutzes vor Schadsoftware sollten Attachments auch clientseitig auf Schadsoftware geprüft werden.
- Beenden des Webmail-Dienstes nur über den vorgesehenen Ausstiegsmechanismus (Log-Out-Button etc.).

13.2.4 Alternative Methoden der Informations- und Datenübertragung

E-Mail ist eine lange etablierte und weit verbreitete Technologie, wurde jedoch ursprünglich nicht für die geschützte Übertragung sicherheitskritischer Daten entwickelt und bietet daher nicht die notwendigen Sicherheits-Features für so einen sicheren Daten- und Informationsaustausch. Durch Verwendung kryptographischer Methoden wie S/MIME kann hier zwar eine Verbesserung erreicht werden, trotzdem bleibt E-Mail eine wenig geeignete Technologie für die Übertragung kritischer und v.a. auch umfangreicher Daten mit hohem Datenvolumen.

Aus diesem Grund werden in diesem Abschnitt mögliche Alternativen zu E-Mail betrachtet, die einen sicheren Datenaustausch auch über Organisationsgrenzen hinaus ermöglichen. Der Fokus liegt dabei auf Methoden der Fernübertragung von Informationen und Daten. Darüber hinaus gehende Varianten des Datenaustauschs beispielsweise mittels der Weitergabe physischer Datenträger (z.B. USB-Sticks) werden hier nicht näher betrachtet.

13.2.4.1 Protokolle zur verschlüsselten Datenübertragung

E-Mail wurde primär für die Übertragung von Textnachrichten konzipiert, dementsprechend ist bei E-Mail die Übertragung von zusätzlichen Daten limitiert und auf die Verwendung von Anhängen/Beilagen (Attachments) beschränkt, für die in der Regel strikte Größenbeschränkungen gelten. Für die Übertragung größerer Datenmengen bieten sich daher explizit dafür ausgelegte Protokolle (bzw. diese Protokolle implementierende Software) an.

Bei der Auswahl entsprechender Software ist auf das zugrundeliegende Protokoll zu achten, da sich für unterschiedliche Protokolle unterschiedliche Sicherheitseigenschaften ergeben:

- **FTP:** Das File Transfer Protocol (FTP) wurde bereits 1985 für die Übertragung von Daten über IP-Netze spezifiziert. FTP bringt keinerlei integrierte Sicherheitsmaßnahmen zur Gewährleistung der Vertraulichkeit, Integrität oder Authentizität von Daten mit und ist für die Übertragung kritischer Daten daher nicht geeignet.
- **SFTP:** Die Abkürzung SFTP steht einerseits für Secure File Transfer Protocol und andererseits für SSH File Transfer Protocol. Dabei handelt es sich um unterschiedliche Protokolle mit unterschiedlichen Sicherheitseigenschaften. Beide Protokolle schützen die Steuerdaten des Übertragungskanals über SSH. Von einer Sicherung der Nutzdaten selbst kann jedoch nicht immer ausgegangen werden. Diese ist nur beim SSH File Transfer Protokoll gegeben, nicht jedoch beim Secure File Transfer Protocol.
- **FTPS:** Beim File Transfer Protocol over SSL (FTPS) werden sämtliche Daten, d.h. auch die Nutzdaten selbst, über SSL/TLS gesichert.

- **SCP:** Secure Copy (SCP) ermöglicht die sichere Übertragung von Daten zwischen zwei Rechnern. Sowohl Steuerdaten als auch die Nutzdaten werden gesichert übertragen.

13.2.4.2 Cloud-Lösungen

Der Austausch von Daten innerhalb einer Organisation aber auch über Organisationsgrenzen hinaus kann auch über diverse Cloud-Lösungen durchgeführt werden. Am Markt existieren diverse Produkte, die eine Datenablage in der Cloud erlauben. Dies erlaubt benutzerfreundliche Datentransfers zwischen Sendern, die Daten in die Cloud hochladen, und Empfängern, die Daten aus der Cloud herunterladen (oder direkt auf den Daten in der Cloud operieren).

Während Cloud-Lösungen definitiv ein benutzerfreundliches Teilen von Daten ermöglichen, müssen bei der Auswahl und Verwendung von Cloud-Lösungen diverse Sicherheitsaspekte berücksichtigt werden. Die zentrale Frage dabei ist, wie die jeweilige Cloud-Lösung konkret umgesetzt ist, d.h. wo die Daten konkret gespeichert werden. Weiters ist auch noch wichtig, welche Schutzfunktionen umgesetzt sind und wie die Authentifizierung am Cloud-Service durchführbar ist.

Populäre und breit verwendete Cloudspeicher-Lösungen wie zum Beispiel Amazon Drive, box, Dropbox, Google Drive und Microsoft OneDrive sind für die Speicherung und den Austausch sicherheitskritischer Daten vor allem im professionellen Umfeld zumeist nicht geeignet. Grund dafür ist die Tatsache, dass bei diesen Lösungen die Daten die jeweilige Organisation verlassen und direkt vom Clouddienstanbieter gespeichert werden. Eine Verwendung solcher Dienste kann für kritische Daten nur dann möglich werden, wenn diese Daten vor dem Hochladen in die Cloud durch den Sender in ausreichender Form verschlüsselt und erst nach dem Download durch den legitimen Empfänger wieder entschlüsselt werden.

Besser geeignet sind hier on-premise Lösungen (Private Cloud), bei denen die Cloud-Infrastruktur direkt in der IT-Infrastruktur der Organisation aufgesetzt wird. Auf diese Weise können Benutzer organisationsintern von den Vorzügen einer Cloud-Lösung profitieren, während die Daten selbst die Organisationsgrenzen nicht verlassen und somit stets unter Kontrolle der Organisation bleiben. Darüber hinaus bieten gängige on-premise Lösungen zudem die Möglichkeit, organisationsfremden Personen kontrollierten, d.h. authentifizierten, Zugang zu ausgewählten Daten zu gewähren oder auch externen Personen die Möglichkeit zu geben, eigene Daten in die on-premise Lösung hochzuladen. Dadurch ermöglichen diese Lösungen auch einen sicheren Datenaustausch über Organisationsgrenzen hinweg.

In jedem Fall ist bei der Verwendung von Cloud-Lösungen sicherzustellen, dass der Abruf von Daten aus der Cloud, die Bereitstellung von Daten in die Cloud oder auch die direkte Bearbeitung von Daten in der Cloud über sichere Client-Programme und Kommunikationsverbindungen vonstatten geht. Wichtig ist dabei sowohl stationäre Geräte (z.B.: PC) und auch mobile Endgeräte zu berücksichtigen. Nur dann ist die Sicherheit der übertragenen bzw. verarbeiteten Daten sichergestellt. Wird beispielsweise als Client-Programm ein Web-Browser verwendet, ist sicherzustellen, dass dieser frei von Schadsoftware ist und mit entfernten zentralen Cloud-Infrastrukturen über gesicherte Verbindungen (HTTPS) kommuniziert.

13.2.4.3 Instant-Messengers und Collaboration-Software

Während erste Instant-Messaging-Lösungen in Form einfacher Chat-Programme bereits vor einigen Jahrzehnten breite Verwendung erfuhren, wurden diese im Laufe der Zeit immer mächtiger und unterstützen heutzutage unter anderem auch den direkten Austausch von Dateien. Da Instant-Messenger und Collaboration-Software auch im professionellen Umfeld zunehmend Verbreitung finden, werden diese mitunter auch für den schnellen und einfachen Austausch von Daten verwendet.

Die Sicherheit der auf diese Weise übertragenen Daten hängt stark von der Implementierung der jeweiligen Lösung ab, sodass allgemeingültige Aussagen an dieser Stelle schwer zu treffen sind. In jedem Fall sollten diese Lösungen mit Bedacht verwendet werden. Bevor diese für die Übermittlung sicherheitskritischer Daten verwendet werden, sollte deren Funktionsweise und deren Sicherheitseigenschaften eingehend evaluiert werden. Im Zweifelsfall – etwa wenn Implementierungsdetails oder unterstützte Sicherheitsfunktionen nicht klar ersichtlich oder überprüfbar sind – sollte von einer Verwendung dieser Lösungen für die Übertragung kritischer Daten abgesehen werden. Generell sollten in den meisten Fällen jedoch sicherheitskritische Daten eher nicht über derartige Messenger verschickt werden.

13.2.4.4 Mobile Messenger-Apps

Auch im professionellen Umfeld kommen vor allem für die interne aber zunehmend auch für die externe Kommunikation immer öfter auch mobile Messenger-Apps wie WhatsApp, Telegram oder Signal zum Einsatz. Auch diese bieten in der Regel die Möglichkeit der direkten Übertragung von Dateien an Kommunikationspartner.

In Bezug auf die Sicherheit dieser Apps und der über diese Apps übertragenen Daten gelten ähnliche Überlegungen wie für Messenger-Lösungen auf klassischen Endnutzergeräten. Allgemeingültige Aussagen sind hier kaum möglich, da die Sicherheit stark von der jeweiligen Lösung abhängt. Auch sind unbedingt eingehende Sicherheitsanalysen notwendig, bevor eine App zum Transfer kritischer Daten verwendet wird. Auch hier sollte im Zweifelsfall von einer Verwendung abgesehen werden.

14 Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems

Der IT-Sicherheitsprozess endet nicht mit der Umsetzung von Maßnahmen. Umfassendes IT-Sicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die IT-Sicherheit im laufenden Betrieb aufrechtzuerhalten. Ein IT-Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden. Weiters muss eine angemessene Reaktion auf sicherheitsrelevante Ereignisse gewährleistet sein.

Ziel aller Follow-Up-Aktivitäten muss es sein, das erreichte Sicherheitsniveau aufrecht zu erhalten bzw. weiter zu erhöhen. Verschlechterungen der Wirksamkeit von Sicherheitsmaßnahmen - sei es durch eine Veränderung der Bedrohungslage oder durch falsche Verwendung der implementierten Sicherheitsmaßnahmen - sollen erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

Die Verantwortlichkeiten für diese Aktivitäten müssen im Rahmen der organisationsweiten IT-Sicherheitspolitik bzw. der einzelnen IT-Systemsicherheitspolitiken festgelegt werden. Als Richtlinie kann auch hier gelten, dass die Verantwortung für systemspezifische Maßnahmen bei den einzelnen Informationssicherheitskoordinatoren im Bereich liegen sollte, die Verantwortung für organisationsweite IT-Sicherheitsmaßnahmen sowie die Gesamtverantwortung bei der bzw. beim Datenschutzbeauftragten/CISO.

Von besonderer Bedeutung für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen MitarbeiterInnen für Fragen der IT-Sicherheit (vgl. dazu auch 7.3 Sicherheitssensibilisierung und -schulung).

Die Anforderungen an die Sicherheit eines IT-Systems sollten bereits zu Beginn der Entwicklung ermittelt und abgestimmt werden. Eine nachträgliche Implementierung von Sicherheitsmaßnahmen ist bedeutend teurer und bietet i. Allg. weniger Schutz als Sicherheit, die von Beginn an in den Systementwicklungsprozess oder in den Auswahlprozess für ein Produkt integriert wurde.

Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Die in 14.1 Sicherheit im gesamten Lebenszyklus eines IT-Systems angeführten Maßnahmen orientieren sich am „Vorgehensmodell für die Entwicklung von IT-Systemen des Bundes“ [IT-BVM] sowie teilweise an den Vorgaben der „Information Technology Security Evaluation Criteria“ [ITSEC] bzw. der [Common Criteria].

Im Gegensatz zu den ITSEC, die zwischen „IT-Systemen“ und „IT-Produkten“ unterscheiden, wobei der gemeinsame Oberbegriff „Evaluierungsgegenstand“ (EVG) lautet, wird in den folgenden Maßnahmenbeschreibungen der besseren Lesbarkeit halber, wenn nicht explizit angeführt, stets von „IT-Systemen“ oder einfach „Systemen“ gesprochen, auch wenn es sich im Einzelfall um ein Produkt (etwa Standardsoftware) oder eine Einzelkomponente handelt.

14.1 Sicherheit im gesamten Lebenszyklus eines IT-Systems

In den [IT-BVM] wird ein an die Bedürfnisse der österreichischen Bundesverwaltung angepasstes Vorgehensmodell (V-Modell) für die Entwicklung von IT-Systemen vorgestellt, das im Folgenden kurz beschrieben wird.

Das österreichische Vorgehensmodell wurde in Anlehnung an das international anerkannte deutsche Vorgehensmodell [Anmerkung: Dieses wird seit vielen Jahren in vielen europäischen Ländern angewendet und wird laufend von der Bundesrepublik Deutschland gewartet und verbessert] entwickelt. Es teilt sich in vier Bereiche auf:

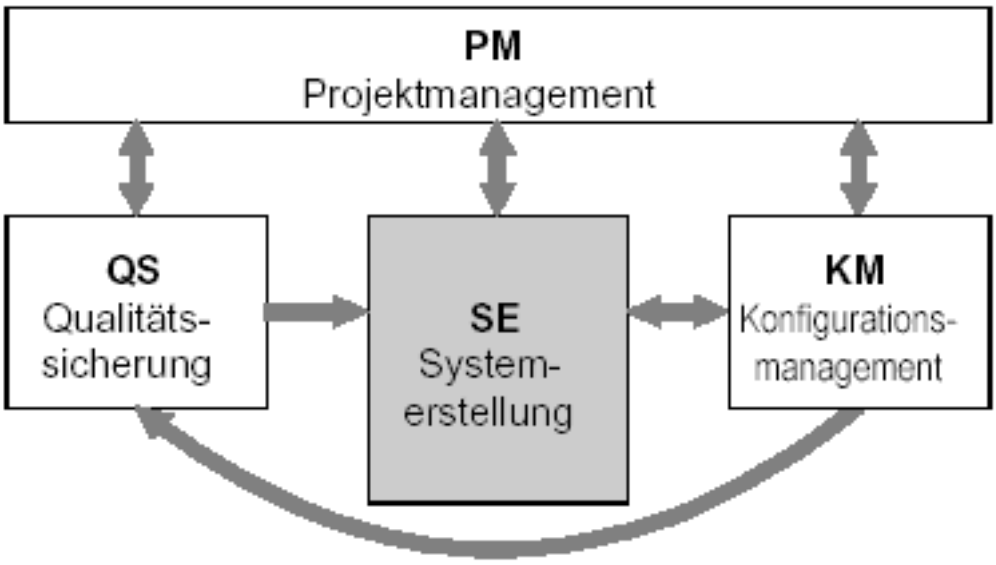

Abbildung 14.1: Die vier Bereiche (Submodelle) des IT-BVM

SE - Systemerstellung

In diesem Bereich werden die Tätigkeiten beschrieben, die zur eigentlichen Erstellung des EDV-Systems notwendig sind. Weiters beschreibt es die Abhängigkeiten der Tätigkeiten untereinander und deren erzeugte Ergebnisse.

PM - Projektmanagement

Hier werden alle Tätigkeiten zusammengefasst, die das Projekt steuern (wie z. B. Kostensteuerung, Terminsteuerung usw.).

QS - Qualitätssicherung

Tätigkeiten, um eine hohe Qualität der EDV-Anwendung sicherzustellen, werden in der QS zusammengefasst.

KM - Konfigurationsmanagement

Dieser Bereich beinhaltet Tätigkeiten, die Änderungen leichter nachvollziehbar bzw. überhaupt erst möglich machen (z. B. die Ablage der Entwicklungsdokumente und des Programmcodes).

Alle diese Bereiche sind eng miteinander verzahnt.

Systemerstellung (SE)

Der Bereich SE gliedert sich in sechs Phasen (Vierecke im Hintergrund). Jede Phase teilt sich in weitere Elementarphasen (Blöcke im Vordergrund) und diese wiederum in Aktivitäten (nicht abgebildet).

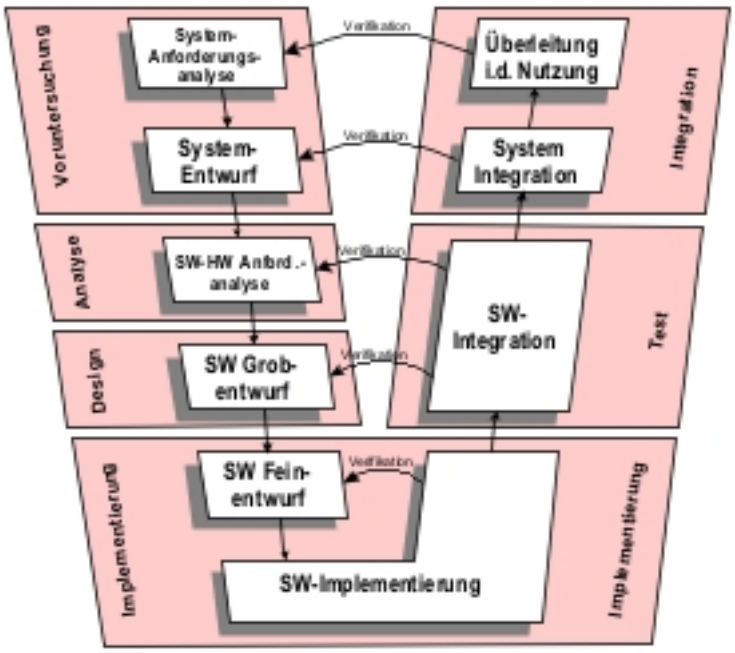

Abbildung 14.2: Gliederung des Vorgehensmodells

Es folgt eine kurze Beschreibung der Elementarphasen:

- SE 1 - Systemanforderungsanalyse:

Hier werden die Anforderungen an das Gesamtsystem erhoben. Unter dem Gesamtsystem versteht man nicht nur das IT-System, sondern auch das fachliche Umfeld, selbst wenn Teile davon später nicht mittels EDV abgedeckt werden.

- SE 2 - Systementwurf:
  Der Grobentwurf des Gesamtsystems wird ermittelt und festgehalten
- SE 3 - SW-/HW-Anforderungsanalyse:
  In dieser Elementarphase konzentriert man sich bereits auf die Anforderungen der Software bzw. der Hardware. Bereiche, die nicht von der späteren IT-Anwendung betroffen sind, werden hier nicht weiter untersucht.
- SE 4 - SW-Grobentwurf:
  Die Software wird grob gegliedert und beschrieben.
- SE 5 - SW-Feinentwurf:
  Die zuvor gebildete grobe SW-Struktur wird weiter verfeinert und beschrieben.
- SE 6 - SW-Implementierung:
  Die Softwarevorgaben werden in Programme bzw. Datenbanken umgesetzt. Erste Überprüfungen gegenüber dem SW-Feinentwurf werden durchgeführt.
- SE 7 - SW-Integration:
  Die einzelnen Softwareteile werden zu größeren Softwareeinheiten zusammengefügt und getestet.
- SE 8 - System integrieren:
  Die Software wird zum Gesamtsystem integriert.
- SE 9 - Überleitung in die Nutzung:
  Das Gesamtsystem (EDV + Infrastruktur) wird am Bestimmungsort installiert und in Betrieb genommen.

Die Reihenfolge der Aktivitäten erscheint sequentiell. Dies entspricht der Vorstellung vom IT-Systemerstellungsprozess als einem strengen Top-down-Vorgehen. In der Regel sind jedoch Iterationen im Erstellungsprozess üblich. Die nachfolgende Abbildung zeigt eine schematisierte linearisierte Darstellung des logischen Ablaufs, der IT-Systemerstellung und deren Einbettung in das organisatorische Umfeld.

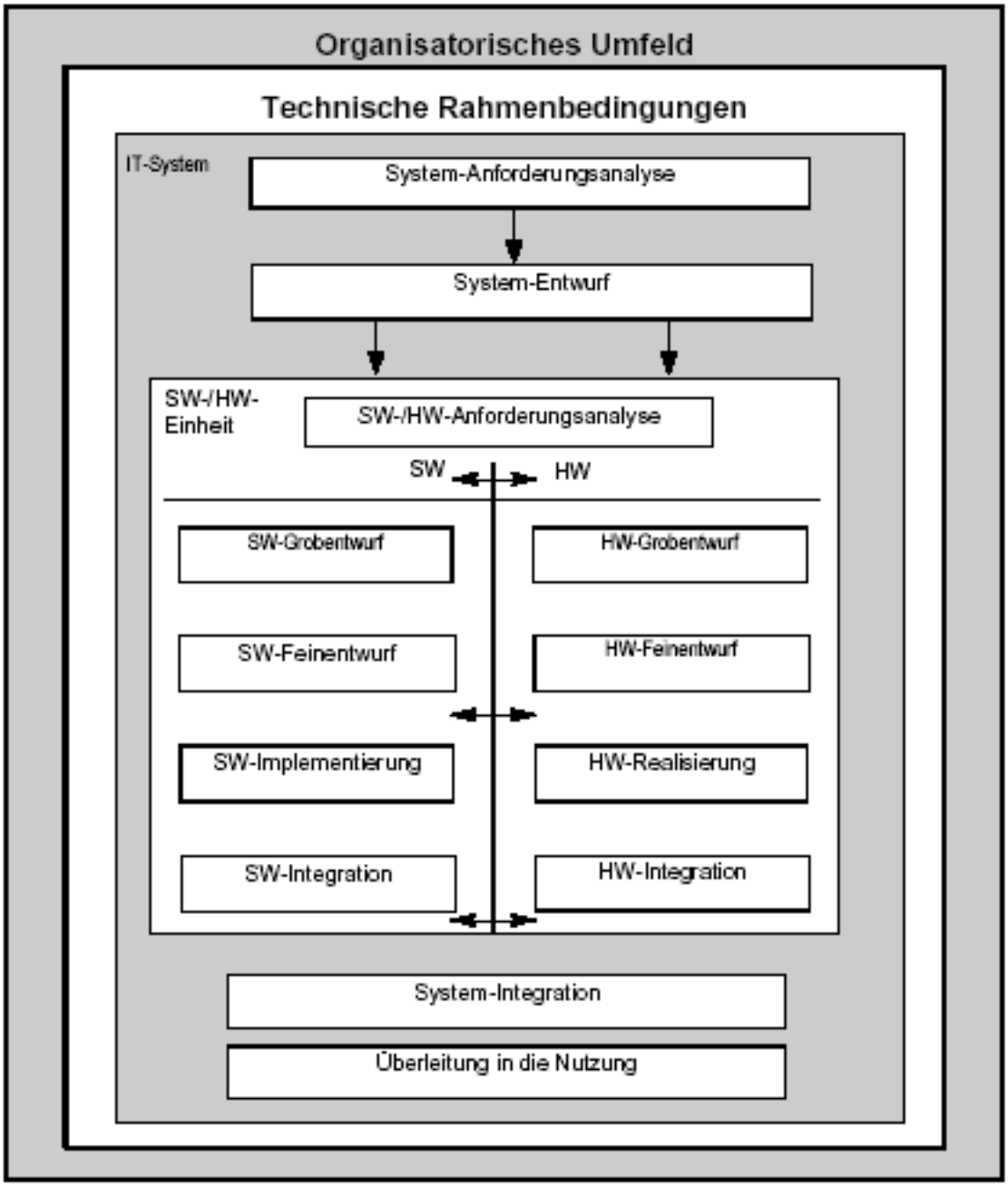

Abbildung 14.3: Randbedingungen zur IT-Systemerstellung

Das beschriebene Vorgehensmodell dient als Grundlage für die nachfolgenden Maßnahmen. Dabei werden die in den einzelnen Phasen für die IT-Sicherheit relevanten Maßnahmen herausgegriffen. Für weitere Details zum Vorgehensmodell sei auf das Gesamtkonzept ([IT-BVM]) verwiesen.

14.1.1 IT-Sicherheit in der Systemanforderungsanalyse

Die Voruntersuchung besteht aus den Elementarphasen „Systemanforderungsanalyse“ und „Systementwurf“, die sich ihrerseits aus unterschiedlichen Aktivitäten zusammensetzen.

In der Systemanforderungsanalyse, der ersten Elementarphase der Phase Voruntersuchung, werden die Anforderungen an das Gesamtsystem erhoben. Unter dem Gesamtsystem versteht man dabei nicht nur das IT-System, sondern auch das fachliche Umfeld, selbst wenn Teile davon später nicht mittels EDV abgedeckt werden.

Der Anforderungskatalog kann etwa Aussagen zu folgenden Punkten enthalten:

- Funktionale Anforderungen,
  die das System zur Unterstützung der Aufgabenerfüllung der Fachabteilung erfüllen muss. Die für die Fachaufgabe relevanten Einzelfunktionalitäten sollten hervorgehoben werden.
- IT-Einsatzumgebung:
  Diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die durch das System an die Einsatzumgebung vorgegeben werden.
- Kompatibilitätsanforderungen
  zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität.
- Performanceanforderungen:
  diese beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.
- Interoperabilitätsanforderungen,
  d. h. die Zusammenarbeit mit anderen Produkten bzw. Systemen über Plattformgrenzen hinweg muss möglich sein.
- Alternativen zu Herstellermonopolen:
  Alternativen zu entstehenden Herstellermonopolen sind im Rahmen der Systemanforderungsanalyse zu berücksichtigen. Speziell im Hinblick auf Kompatibilität und Austauschbarkeit im Notfall ist dies ein Beitrag zur Systemsicherheit. Als eine der Hauptschwierigkeiten wären beispielsweise proprietäre Protokolle zu identifizieren, die Probleme bei der Suche nach Ersatzsystemen darstellen. Aufgrund des IKT-Board-Beschlusses [IKTB-250602-1] sind derartige Alternativen bei Anschaffungen von Servern im Rahmen der öffentlichen Verwaltung empfohlen (vgl. auch K-Fall-Vorgaben in 17.1.1 Definition von Verfügbarkeitsklassen).
- Zuverlässigkeitsanforderungen:
  Diese betreffen die Stabilität des Systems, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.

- Konformität zu Standards:
  Dies können internationale Normen, De-facto-Standards oder auch Hausstandards sein.
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften,
  z. B. ausreichender Datenschutz bei der Verarbeitung personenbezogener Daten.
- Anforderungen an die Benutzerfreundlichkeit,
  insbesondere an die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen.
- Anforderungen an die Wartbarkeit.
- Obergrenze der Kosten:
  Dabei müssen nicht nur die unmittelbaren Entwicklungs- bzw. Beschaffungskosten für das System selbst einbezogen werden, sondern auch Folgekosten, wie z. B. Wartungsaufwände, Personalkosten oder notwendige Schulungen.
- Aus den Anforderungen an die Dokumentation muss hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.
- Bezüglich der Softwarequalität können Anforderungen gestellt werden, die von Herstellererklärungen über die eingesetzten Qualitätssicherungsverfahren, über ISO 9000 Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO 12119 reichen.

Zusätzlich zu den operationellen Anforderungen müssen die IT-Sicherheitsziele vorgegeben werden. Dies kann auf zwei Arten erfolgen:

- durch die Formulierung von Anforderungen an Vertraulichkeit, Integrität oder Verfügbarkeit (vgl. 17.1.1 Definition von Verfügbarkeitsklassen) von bestimmten operationellen Funktionen oder verarbeiteten Informationen,
- anhand einer bereits vorgegebenen Sicherheitspolitik, die im Gesamtsystem durchgesetzt werden soll.

Bei der Entwicklung von KI-Systemen ist auf deren besonderen Anforderungen Rücksicht zu nehmen. So sollten KI-Systeme beispielsweise hinreichend neutral trainiert werden und resistent gegenüber Angriffen sein, bei denen manipulierte Daten in das Datenmodell eingeschleust oder Daten daraus extrahiert werden können, wodurch die IT-Sicherheitsziele Vertraulichkeit, Integrität und auch Verfügbarkeit beeinträchtigt würden.

14.1.2 Durchführung einer Risikoanalyse und Festlegung der IT-Sicherheitsanforderungen

Basierend auf den bereits definierten Anwenderanforderungen und Informationen über die Einsatzumgebung des Systems sind die für das System relevanten Bedrohungen zu ermitteln und die damit verbundenen Risiken zu bewerten.

Zu möglichen Strategien und Vorgehensweisen zur Risikoanalyse siehe 4 Informationssicherheitspolitik.

Die Ergebnisse der Risikoanalyse bilden die Grundlage für die Formulierung der Anforderungen an die IT-Sicherheit innerhalb der Anwenderforderungen (vgl. 14.1.1 IT-Sicherheit in der Systemanforderungsanalyse).

Typische **Sicherheitsanforderungen,** die an ein gesamtes IT-System oder auch an eine Einzelkomponente oder ein Produkt möglicherweise gestellt werden, seien im Folgenden kurz erläutert (dabei wird im Folgenden wieder generell von „Systemen“ gesprochen). Weitere Ausführungen finden sich in den „Information Technology Security Evaluation Criteria“ [ITSEC] und den [Common Criteria].

- Identifizierung und Authentisierung:
  In vielen Systemen wird es Anforderungen geben, diejenigen BenutzerInnen zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom System kontrolliert werden. Dazu muss nicht nur die behauptete Identität der BenutzerInnen festgestellt, sondern auch die Tatsache nachgeprüft werden, dass die BenutzerInnen tatsächlich die Personen sind, die sie zu sein vorgeben. Dies geschieht, indem die BenutzerInnen dem System Informationen lieferen, die fest mit den betreffenden BenutzerInnen verknüpft sind. Dies können entweder personenbezogene oder personengebundene Informationen sein, siehe dazu auch 9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung.
- Zugriffskontrolle:
  Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass BenutzerInnen und Prozesse daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung, Änderung oder Löschung von Informationen geben.
- Beweissicherung:
  Bei vielen Systemen wird es erforderlich sein sicherzustellen, dass über Handlungen, die von BenutzerInnen bzw. von Prozessen im Namen solcher BenutzerInnen ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später den betreffenden BenutzerInnen zugeordnet werden können und die BenutzerInnen für ihre Handlungen verantwortlich gemacht werden können.
- Protokollauswertung:
  Bei vielen Systemen wird sicherzustellen sein, dass sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.
- Unverfälschbarkeit:

Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und dass Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden. Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, BenutzerInnen und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.

- Zuverlässigkeit:
  Bei vielen Systemen wird es erforderlich sein, sicherzustellen, dass zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Systemen erforderlich sein, sicherzustellen, dass ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.
- Übertragungssicherung:
  Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind:
  - Authentisierung
  - Zugriffskontrolle
  - Datenvertraulichkeit
  - Datenintegrität
  - Sende- und Empfangsnachweis

Über die „Information Technology Security Evaluation Criteria“ [ITSEC] hinaus können weitere Sicherheitsanforderungen bestehen, wie etwa Datensicherung, Verschlüsselung gespeicherter Daten, Funktionen zur Wahrung der Datenintegrität oder datenschutzrechtliche Anforderungen.

Die speziellen Risiken von KI-Systemen erfordern eine darauf abgestimmte systematische Risikoanalyse. Ein Fokus sollte dabei auf neuartige Angriffe und spezifische Bedrohungen gelegt werden, vor allem auf das Extrahieren von Modelldaten einer KI oder auch den angewendeten Algorithmen. Falls Betriebsdaten des KI-Systems wiederum in die Trainingsdaten einfließen, müssen Angriffe mit dem Ziel einer Datenmanipulation betrachtet werden. Ebenso sind dadurch Adversariale Angriffe möglich, bei denen durch Manipulation der Eingabedaten versucht wird nicht vorhergesehene Ausgaben zu erzwingen. Es ist daher essenziell die KI über den gesamten Lebenszyklus auf die korrekte Funktionalität und Robustheit gegenüber Angriffen zu kontrollieren.

Stärke der Mechanismen

[Common Criteria] definiert eine Stärke der Funktion (Strength of Function – SOF). Es handelt sich dabei um eine Charakterisierung von Sicherheitsfunktionen des Produkts, die den geringsten angenommenen Aufwand beschreibt, um die zugrunde liegenden Sicherheitsmechanismen durch einen direkten Angriff außer Kraft zu setzen. Es werden drei Stufen über das Angriffspotenzial definiert:

- niedrig:
  Die Stufe bietet angemessenen Schutz gegen zufälliges Brechen der Sicherheit durch AngreiferInnen, die über ein geringes Angriffspotenzial verfügen.
- mittel:
  Die Stufe bietet einen angemessenen Schutz gegen nahe liegendes oder absichtliches Brechen durch AngreiferInnen, die über ein mittleres Angriffspotenzial verfügen.
- hoch:
  Die Stufe bietet einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch AngreiferInnen, die über ein hohes Angriffspotenzial verfügen.

Ähnlich werden in den „Information Technology Security Evaluation Criteria“ [ITSEC] drei Stufen (niedrig, mittel, hoch) für die Stärke des Mechanismus definiert.

14.1.3 IT-Sicherheit in Design und Implementierung

Systementwurf:

> *Diese Elementarphase des Entwicklungsprozesses bezieht sich auf die oberste Stufe der Definition und des Entwurfs eines IT-Systems oder Produktes. Dies erfolgt in Form einer Spezifikation auf hohem Abstraktionsniveau, die die grundlegende Struktur des Systems, seine externen Schnittstellen sowie seine Untergliederung in die wichtigsten Hardware- und Softwarekomponenten identifiziert.*

Bereits in dieser Elementarphase, in der die Systemarchitektur und ein Integrationsplan erarbeitet werden, ist auf eine adäquate Berücksichtigung der Sicherheitsanforderungen zu achten.

Aus Sicht der IT-Sicherheit ist es insbesondere wichtig, dass bereits im Systementwurf eine klare und wirksame Trennung zwischen IT-sicherheitsspezifischen, IT-sicherheitsrelevanten und anderen Komponenten getroffen wird. Eine klare Trennung unterstützt die Sicherstellung der Korrektheit der weiteren Entwicklungsschritte und erleichtert eine eventuelle Evaluierung der Sicherheit des Systems (etwa nach den „Information Technology Security Evaluation Criteria“ [ITSEC] oder [Common Criteria]).

Dabei bedeuten:

- IT-sicherheitsspezifische Komponenten:
  Komponenten, die unmittelbar zur Durchsetzung der IT-Sicherheit beitragen
- IT-sicherheitsrelevante Komponenten:
  Komponenten, die nicht unmittelbar zur IT-Sicherheit beitragen, deren Fehlverhalten oder Missbrauch jedoch die Sicherheit gefährden kann.

Die Schnittstellen der IT-Sicherheitsmaßnahmen zu den beteiligten Architekturelementen müssen dokumentiert werden.

SW-Grobentwurf und SW-Feinentwurf:

Diese Elementarphasen des Entwicklungsprozesses beziehen sich auf die Verfeinerung des Systementwurfes bis hin zu einem Detaillierungsgrad, der als Basis für die Programmierung (oder die Hardwarekonstruktion) verwendet werden kann.

Aus Sicht der IT-Sicherheit sind hier insbesondere

- die Abhängigkeiten der IT-Sicherheitsfunktionen,
- die Wechselwirkungen der IT-Sicherheitsmechanismen, die zur Realisierung der IT-Sicherheitsfunktionen gewählt wurden, und
- die Auswirkungen, die die Realisierung der IT-Sicherheitsfunktionen auf andere SW-Einheiten haben können

zu untersuchen.

Alle Schnittstellen der IT-sicherheitsspezifischen und der IT-sicherheitsrelevanten SW-Komponenten und -Module müssen mit ihrem Zweck und ihren Parametern beschrieben werden. Die Separierung vom nicht IT-sicherheitsrelevanten Teil muss sichtbar sein.

Weiters ist festzustellen, ob und gegebenenfalls welche IT-sicherheitsspezifischen oder IT-sicherheitsrelevanten Anteile in anderen SW-Komponenten, -Modulen bzw. Datenbanken bei der Realisierung entstehen.

Implementierung und Tests:

Jede Komponente bzw. jedes Modul ist zunächst aus den Spezifikationen zu programmieren oder zu konstruieren. Diese Komponenten und Module müssen dann gegen ihre Spezifikationen geprüft und getestet werden. Anschließend werden einzelne Komponenten und Module zusammen in kontrollierter Form integriert, bis das komplette System vorliegt, das dann als Ganzes gegen die Spezifikation und die Sicherheitsvorgaben geprüft und getestet wird (vgl. dazu [IT-BVM], Kapitel 7, 8 und 9 (Phasen Implementierung, Test und Integration)). Details dazu siehe auch 14.1.5 Entwicklung eines Testplans für Standardsoftware und 14.1.6 Testen von Software.

14.1.4 Entwicklungsumgebung

Zur Entwicklungsumgebung zählen Maßnahmen, Verfahren und Standards, die während der Systemerstellung zum Einsatz kommen.

Zur Gewährleistung der Sicherheit des zu entwickelnden Systems sind auch an die Sicherheit der Entwicklungsumgebung besondere Anforderungen zu stellen. Abhängig von den Sicherheitsanforderungen an das System und den Anforderungen in dessen Vertrauenswürdigkeit können dies etwa sein:

Konfigurationskontrolle

Die Konfigurationskontrolle soll sicherstellen, dass alle Entwurfsergebnisse und Implementierungen in kontrollierter Form erstellt und geändert werden und dass sie nachweislich den früheren Darstellungen entsprechen.

Es ist wichtig, dass alle Versionen eines Systems eindeutig (z. B. durch Versionsnummern) identifiziert werden können. In vielen Fällen wird es sinnvoll sein, den Entwicklungsvorgang durch ein Konfigurationskontrollsystem zu unterstützen. [Common Criteria] fordert etwa einen Konfigurationsmanagement-Plan ab Evaluationsstufe EAL3 (Evaluation Assurance Level), automatisiertes Konfigurationsmanagement ab Evaluationsstufe EAL4.

Sicherheit bei den EntwicklerInnen

Es ist sicherzustellen, dass die Entwicklung gegen böswillige Angriffe geschützt ist und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewährleistet sind (vgl. dazu § 126a Datenbeschädigung (StGB)).

Dazu ist eine Reihe von organisatorischen, technischen und personellen Maßnahmen erforderlich, die im Detail in anderen Maßnahmenbeschreibungen in diesem Handbuch nachgelesen werden können.

Grundsätzlich zu beachten sind dabei unter anderem:

- Die physische Sicherheit der Räume und Gebäude, in denen die Entwicklung erfolgt (Zutrittskontrolle, Einbruchs- und Brandschutz, …, vgl. 11.1 Bauliche und infrastrukturelle Maßnahmen).
- Personelle Sicherheit:
  Bei der Entwicklung sicherheitsrelevanter bzw. sicherheitsspezifischer Systeme und Komponenten darf nur vertrauenswürdiges Personal zum Einsatz kommen.
- Sicherheit bei der Übertragung von Informationen und der Übersendung von Datenträgern:
  Abhängig von den Vertraulichkeitsanforderungen sind entsprechende Maßnahmen zum Schutz der Informationen zu treffen.

- Sicherstellung der Verfügbarkeit der Ergebnisse (vgl. 17 Disaster Recovery und Business Continuity).

Trennung von Entwicklungs- und Produktionsumgebung

Es ist eine strikte Trennung der Entwicklungs- von der Produktionsumgebung vorzusehen.

Auch die Produktion ist, wie die Entwicklung, gegen Angriffe sowohl von InsiderInnen als auch von AußentäterInnen zu schützen.

Es empfiehlt sich, die Anforderungen und Maßnahmen zur Gewährleistung der Sicherheit in der Entwicklungsumgebung in einem eigenen Dokument festzuhalten.

14.1.5 Entwicklung eines Testplans für Standardsoftware

Sowohl bei der Eigenentwicklung von IT-Systemen als auch beim Einsatz von Produkten (Standardsoftware) sind ausführliche Tests unumgänglich. Während im Rahmen der Eigenentwicklung Tests den gesamten Entwicklungsprozess begleiten (vgl. Regelwerk SE im [IT-BVM]), muss Standard-SW im Rahmen des Auswahlprozesses ausführlich getestet werden.

Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und andere Freigabebedingungen.

Die im Nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken [ISO/IEC 12119] („Softwareerzeugnisse, Qualitätsanforderungen und Prüfbestimmungen“), Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik ([ITSEM]).

Um sicherzugehen, dass das Produkt die gestellten Anforderungen auch im gewünschten Maße erfüllt, sind systematische Tests zur Überprüfung der Eignung und Zuverlässigkeit auf Grundlage des Anforderungskataloges erforderlich.

Dabei bietet es sich an, das Testen in vier Bereiche einzuteilen:

- Eingangsprüfungen (Prüfung auf Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, …),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),
- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation) und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Es ist ein Testplan zu erstellen, der folgende Inhalte umfasst:

- Festlegung der Testinhalte anhand des Anforderungskataloges,
- Überprüfung von Referenzen, gegebenenfalls Berücksichtigung eventuell vorhandener Zertifizierungsreports,
- Festlegung des Gesamtprüfaufwandes,
- Zeitplanung einschließlich Prüfaufwand je Testinhalt,
- Festlegung der Testverantwortlichen,
- Testumgebung,
- Inhalt der Testdokumentation,
- Festlegung von Entscheidungskriterien.

Anforderungen an die Testumgebung:

- Die Virenfreiheit der Testumgebung ist durch ein aktuelles Virensuchprogramm sicherzustellen.
- Die Testumgebung muss frei sein von Seiteneffekten auf den Echtbetrieb. Um Wechselwirkungen von vornherein zu vermeiden, empfiehlt es sich, dedizierte IT-Systeme zu installieren.
- Die Zugriffsrechte müssen in der Testumgebung derart konfiguriert werden, wie sie dem Produktionsbetrieb entsprechen.
- Der Zutritt und Zugang zur Testumgebung muss geregelt sein.
- Es muss sichergestellt werden, dass das Produkt genau in der Konfiguration in den Produktionsbetrieb übernommen wird, die in der Testumgebung ermittelt wurde. Daher ist in der Testumgebung ein geeignetes Verfahren zum Integritätsschutz einzusetzen (etwa digitale Signaturen oder kryptographische Checksummen).
- Die Kosten für den Aufbau der Testumgebung müssen angemessen sein.

Wird beim Testen ein automatisiertes Werkzeug verwendet, muss die Testdokumentation ausreichende Informationen über dieses Werkzeug und die Art seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.

14.1.6 Testen von Software

Das Testen von Software lässt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen.

In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

Testvorbereitung:

- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)

- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

Testdurchführung:

- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung (Einsatz unter Echtbedingungen), falls erforderlich

Testauswertung:

- Bewertung der Testergebnisse anhand festgelegter Entscheidungskriterien
- Zusammenführung der Ergebnisse
- Dokumentation

Aus Sicht der IT-Sicherheit sind insbesondere auch folgende Aspekte zu untersuchen (sicherheitsspezifische Tests):

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik ([ITSEM]) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweisen beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.

Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen.

Zum Testen von Anwendungen, die auf die Bürgerkartenfunktionalität zugreifen, soll auf nicht real existente Testpersonen, die im ZMR für diesen Zweck formell eingerichtet wurden, zurückgegriffen werden [IKTB-220905-01] .

Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen, sind Penetrationstests durchzuführen. Diese sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potenzielle Schwachstellen ergeben können. Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.

Penetrationstests können durch die Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch potenzielle AngreiferInnen zur Ausnutzung von Schwachstellen benutzen würden, wie z. B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,
- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Weiters ist die Stärke der Mechanismen zu überprüfen (vgl. dazu 14.1.2 Durchführung einer Risikoanalyse und Festlegung der IT-Sicherheitsanforderungen).

Es muss sichergestellt werden, dass die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, dass durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern.

14.1.7 Abnahme und Freigabe von Software

Sowohl Standardsoftware als auch selbst- oder im Auftrag entwickelte Programme müssen einer geregelten Abnahme und Freigabe unterzogen werden (vgl. dazu auch Kapitel 9 (Phase Integration) des Regelwerks SE des IT-BVM [IT-BVM]).

In der **Abnahme** sollte überprüft werden, ob die Software

- die erforderliche Funktionalität zuverlässig bereitstellt,
- keine nicht dokumentierten Funktionen enthält,
- frei von Viren ist (insbesondere bei Standardsoftwareprodukten),
- kompatibel zu den anderen eingesetzten Produkten ist,
- in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind.

Im Falle von Standardsoftware ist darüber hinaus zu prüfen, ob diese komplett einschließlich der erforderlichen Handbücher/Dokumentationen ausgeliefert wurde, für Eigenentwicklungen ist die Vollständigkeit und Korrektheit der Dokumentation zu prüfen. Näheres zu den Anforderungen an die Dokumentation siehe 12.2.1 Dokumentation von Software.

Abnahmeplan:

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- Die Testfälle werden von der fachlich zuständigen Stelle entwickelt.
- Für Testfälle werden keine Daten des Echtbetriebs benutzt.
- Testdaten, insbesondere wenn sie durch Kopieren der Echtdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren.
- Die Durchführung der Tests darf keine Auswirkungen auf den Echtbetrieb haben. Nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn

- schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen,
- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind oder
- die Dokumentation der Software nicht vorhanden oder nicht ausreichend ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

Freigabe:

Ist die Abnahme der Software erfolgt, muss die Software für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- Installationsanweisungen,
- evtl. Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis, …),
- evtl. erforderliche Schulungen,
- Freigabedatum, ab wann die Software eingesetzt werden darf, und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich muss verhindert werden, dass Software nach der Freigabe verändert oder manipuliert werden kann (siehe 14.1.9 Sicherstellen der Integrität von Software). Andernfalls ist dies durch eine Regelung festzulegen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall sind detaillierte Verfahrensweisen festzulegen (AnsprechpartnerIn, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

14.1.8 Installation und Konfiguration von Software

Die freigegebene Software wird entsprechend der Installationsanweisung auf den dafür vorgesehenen IT-Systemen installiert. Die Installationsanweisung beinhaltet neben den zu installierenden Programmen auch Konfigurationsparameter und die Einrichtung der Hardware- und Softwareumgebung.

Abweichungen von der Installationsanweisung bedürfen der Zustimmung der Freigabeinstanz.

Wenn die BenutzerInnen die Software selbst installieren sollen, muss ihnen eine Installationsanweisung zur Verfügung gestellt werden, die eine selbstständige Installation ermöglicht. Mindestens die Pilotinstallation durch ausgewählte typische BenutzerInnen sollte durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Die erfolgreiche Installation wird schriftlich an die für die Aufnahme des Produktionsbetriebes zuständige Stelle gemeldet.

14.1.9 Sicherstellen der Integrität von Software

Es ist sicherzustellen, dass die freigegebene Software nur unverändert installiert werden kann. Damit soll verhindert werden, dass zwischenzeitlich gewollte oder ungewollte Veränderungen vorgenommen werden können, z. B. durch Viren, Bit-Fehler aufgrund technischer Fehler oder Manipulationen in Konfigurationsdateien.

Die Installation darf daher ausschließlich von Originaldatenträgern bzw. von nummerierten Kopien der Originaldatenträger erfolgen. Eine Alternative zur lokalen Installation von Datenträgern ist die Installation einer dafür freigegebenen Version über ein lokales Netz. Dabei ist sicherzustellen, dass nur berechtigte Personen darauf Zugriff haben.

Von den Originaldatenträgern sollten, falls der Datenumfang es zulässt, Sicherungskopien angefertigt werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden. Die angefertigten Kopien sollten nummeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sind zu löschen bzw. zu vernichten.

Vor der Installation muss eine Virenprüfung durchgeführt werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme (vgl. 10.1 Kryptographische Maßnahmen) gebildet werden, anhand derer vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen überprüft werden kann. Darüber hinaus können installierte Programme zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration zusätzlich mit Checksummen versehen werden. Dies ermöglicht es auch, Infektionen mit bisher unbekannten Viren zu erkennen und festzustellen, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

14.1.10 Lizenzverwaltung und Versionskontrolle von Standardsoftware

Ohne geeignete Versions- und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen evtl. einige ohne Lizenz benutzt werden.

Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muss allen MitarbeiterInnen bekannt gemacht werden, die AdministratorInnen der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet werden.

Häufig werden in einer Institution verschiedene Versionen einer Standardsoftware eingesetzt. Im Rahmen der Lizenzkontrolle muss es auch möglich sein, einen Überblick über alle eingesetzten Versionen zu erhalten. Damit kann gewährleistet werden, dass alte Versionen durch neuere ersetzt werden, sobald dies notwendig ist, und dass bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

14.1.11 Deinstallation von Software

Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind, und alle Einträge in Systemdateien, die bezüglich dieser Software vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert.

Um eine vollständige Deinstallation durchführen zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen festzuhalten, entweder manuell oder mit Hilfe von speziellen Tools. Wird dies nicht vorgenommen, kommt es erfahrungsgemäß dazu, dass eine Deinstallation nur rudimentär stattfindet oder dass sie unterlassen wird aus Furcht, wichtige Dateien bei der Deinstallation zu löschen.

Weiters sollte sichergestellt werden, dass bei einer Deinstallation auch alle Vorgängerversionen vollständig deinstalliert werden.

14.2 Evaluierung und Zertifizierung

14.2.1 Beachtung des Beitrags der Zertifizierung für die Beschaffung

Die BenutzerInnen von IT-Systemen müssen sich auf die Sicherheit jedes von ihnen verwendeten Systems verlassen können. Sie benötigen auch einen Maßstab für den Vergleich der Sicherheitseigenschaften von IT-Produkten, deren Anschaffung sie in Betracht ziehen. Neben der Durchführung eigener eingehender Tests oder dem Vertrauen in die Aussagen des Herstellers bzw. Vertreibers wird zunehmend auf die Möglichkeit einer Prüfung und Bewertung durch eine neutrale, vertrauenswürdige Instanz zurückgegriffen. Insbesondere bei einem hohen oder sehr hohen Schutzbedarf kann die Vertrauenswürdigkeit der Produkte in Hinblick auf IT-Sicherheit nur dadurch gewährleistet werden, dass unabhängige Prüfstellen die Produkte untersuchen und bewerten.

Eine solche Evaluation von Systemen oder Produkten erfordert objektive und genau definierte Kriterien für die Bewertung der Sicherheit und das Vorhandensein einer Zertifizierungsstelle, die bestätigen kann, dass die Evaluation ordnungsgemäß durchgeführt wurde.

Eine allgemein anerkannte Grundlage dieser Evaluierungen bilden die europaweit harmonisierten „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ [ITSEC] und das zugehörige Evaluationshandbuch [ITSEM] sowie die weltweit abgestimmten „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria) [Common Criteria].

Aus einem nach der Evaluierung erstellten Zertifizierungsreport geht hervor, welche Funktionalität mit welcher Prüftiefe untersucht wurde und welche Bewertung vorgenommen wurde. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß darstellt für den Aufwand, den man zum Überwinden der Sicherheitsfunktionen aufbringen muss.

Die „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ [ITSEC] kennen etwa die Evaluationsstufen E1 (geringste Prüftiefe) bis E6 (höchste Prüftiefe) und unterscheiden die Mechanismenstärken niedrig, mittel und hoch. Die [Common Criteria] unterscheiden sieben Vertrauenswürdigkeitsstufen (EAL1 bis EAL7), wobei EAL1 unter E1 anzusetzen ist, um den Zugang zur Evaluation zu erleichtern. Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz eines Produktes beachtet werden müssen.

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, so kann ein eventuell vorhandenes Sicherheitszertifikat bzw. Gütesiegel als Auswahlkriterium positiv berücksichtigt werden.

14.3 Einsatz von Software

14.3.1 Nutzungsverbot nicht freigegebener Software

Um sicherzustellen, dass keine Programme mit unerwünschten Auswirkungen eingebracht werden und das System nicht über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen nicht freigegebener Software in Produktionssysteme bzw. ihre Nutzung verboten und - soweit technisch möglich - verhindert werden.

Dabei ist zu beachten:

- Das Nutzungsverbot nichtfreigegebener Software sollte schriftlich fixiert werden, alle MitarbeiterInnen sind darüber zu unterrichten.
- Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.
- Das unautorisierte Einspielen oder Nutzen von Software ist soweit möglich mit technischen Mitteln zu verhindern.
- Es ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden; dabei sind insbesondere Erstellungsdatum und Dateigröße festzuhalten.
- Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

14.3.2 Nutzungsverbot privater Hard- und Softwarekomponenten

I. Allg. sollte ein Nutzungsverbot privater Software (vgl. auch 14.3.1 Nutzungsverbot nicht freigegebener Software), Hardware (Smartphone, USB-Sticks, PC, Notebook) und Daten ausgesprochen werden.

Auch bei Fernzugängen (remote access) ist das Verwendungsverbot privater HW und SW zu beachten (vgl. 13.1.10 Remote Access).

Ausnahmeregelungen (etwa wenn Datenabgleich mit privaten Mobiltelefonen zugelassen wird) sollten einen Erlaubnisvorbehalt vorsehen.

14.3.3 Überprüfung des Softwarebestandes

Um Verstöße gegen das Verbot der Nutzung nicht freigegebener Software feststellen zu können, ist eine regelmäßige Überprüfung des Softwarebestandes notwendig. Ist die Zahl der IT-Systeme sehr groß, kann eine stichprobenartige Überprüfung durchgeführt werden. Die Ergebnisse der Überprüfung sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Dabei ist zu beachten:

- Sollte bei der Überprüfung nicht freigegebene Software gefunden werden, so ist die Legalisierung oder Entfernung zu veranlassen. Es muss festgelegt sein, was mit allfälligen Daten zu geschehen hat, welche mittels illegaler Software verarbeitet bzw. gespeichert wurden.
- Um diese Überprüfung durchführen zu können, muss der überprüfenden Instanz die entsprechende Befugnis durch die Unternehmens- bzw. Behördenleitung verliehen werden.
- Der prüfenden Instanz muss bekannt sein, welche Software auf welchem IT-System freigegeben ist (Softwarebestandsverzeichnis).
- Es ist festzulegen, wie bei Feststellung eines Verstoßes verfahren wird.

14.3.4 Update von Software

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden.

Ein Update ist insbesondere dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Systems haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Vor einem Update sind die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau zu prüfen. Dies geschieht am sinnvollsten auf einem eigenen Testsystem, bevor das Update in den produktiven Einsatz übernommen wird.

Insbesondere ist darauf Bedacht zu nehmen, dass in der Vorgängerversion explizit behobene Sicherheitsmängel nicht wieder neu auftauchen, bzw. getroffene Parametrisierungen nachgezogen werden.

Updates und sicherheitsrelevante Patches werden in der Regel durch den Hersteller bei Bedarf zur Verfügung gestellt. Es ist dabei zu beachten, dass derartige Updates und Patches unbedingt nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Die Authentizität der Quelle ist nach Möglichkeit zu prüfen (beispielsweise anhand vorhandener Serverzertifikate).

14.3.5 Update/Upgrade von Soft- und Hardware im Netzbereich

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Dies betrifft beispielsweise die Betriebssoftware von aktiven Netzkomponenten wie z. B. Switches oder Routern, aber auch eine Netzmanagementsoftware. Ein Update ist insbesondere dann notwendig, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Netzes haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Auch ein Upgrade von Hardware kann in bestimmten Fällen sinnvoll sein, wenn z. B. eine neue Version eines Switches eine höhere Transfer- und Filterrate bietet. Durch diese Maßnahmen kann der Grad der Verfügbarkeit, der Integrität und der Vertraulichkeit unter Umständen erhöht werden.

Bevor ein Upgrade oder ein Update vorgenommen wird, müssen die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht am sinnvollsten in einem physikalisch separaten Testnetz, bevor das Update oder Upgrade in den produktiven Einsatz übernommen wird.

14.3.6 Softwarepflege- und -änderungskonzept

Unter Softwarepflege und -änderung sind alle Maßnahmen zu verstehen, die ergriffen werden,

- um eine zur Benutzung freigegebene Programmausstattung funktionsfähig zu erhalten, ohne dass Spezifikationen geändert oder erweitert werden (Softwarepflege),
- um eine Änderung oder Erweiterung der Spezifikationen in einer zur Benutzung freigegebenen Programmausstattung zu berücksichtigen (Softwareänderung)

(Definition lt. [IT-BVM]).

In den [IT-BVM] werden die inhaltlichen Anforderungen an ein Softwarepflege- und -änderungskonzept (SWPÄ) gegeben.

Diese umfassen u. a.

- Beschreibung der SWPÄ-Organisation (SWPÄ-Team, Aufgaben und Verantwortlichkeiten)

- Beschreibung des SWPÄ-Prozesses (Beantragung, Analyse und Klassifikation von Änderungen, Konfigurationsverwaltung, Verteilung von Datenträgern, Installation)
- Planung der SWPÄ-Bereitschaft (Schaffung der personellen und technischen Voraussetzungen, Ausbildung, entwicklungsbegleitende Maßnahmen)

14.4 Korrekte Verarbeitung

14.4.1 Verifizieren der zu übertragenden Daten vor Weitergabe

Vor dem Versenden einer Datei per E-Mail oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem WWW- oder FTP-Server sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standardsoftware wie z. B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen der BenutzerInnen gespeichert.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde. Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr.

Um Restinformationen zu beseitigen,

- kann die Datei in einem anderen Dateiformat abgespeichert werden, z. B. als „Nur-Text“ oder als HTML,
- können die Nutzdaten in eine zweite Instanz derselben Standardsoftware kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Verborgener Text/Kommentare

Eine Datei kann Textpassagen enthalten, die als „versteckt“ oder „verborgen“ formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für die EmpfängerInnen bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

Änderungsmarkierungen

Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

Versionsführung

Bei einer Vielzahl von Anwendungen gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in *einer* Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z. B. wenn Grafiken mitgeführt werden. Es ist darauf zu achten, dass keine Optionen, die sämtliche Vorgängerversionen automatisch abspeichern, in den Grundeinstellungen der Anwendung ausgewählt werden.

Dateieigenschaften

Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei einer späteren Suche helfen sollen, Dateien wieder zu finden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, BearbeiterInnen (nicht nur die/der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selbst angelegt und können nicht durch die BearbeiterInnen beeinflusst werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

Schnellspeicherung

Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.

Entscheiden sich die BenutzerInnen trotzdem für die Schnellspeicheroption, sollten sie bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

14.5 Sicherheit von Systemdateien

14.5.1 Systemdateien

Das unbeabsichtigte und unkundige Ändern bzw. Löschen von Systemdateien kann verheerende Auswirkungen auf die Stabilität und Zuverlässigkeit des IT-Systems haben. Eine strikte Rechtevergabe bei diesen Dateien ist daher besonders zu empfehlen.

I. Allg. sollte nur AdministratorInnen der Zugriff auf diese Dateien gewährt werden. Darüber hinaus ist eine regelmäßige Verifizierung der Integrität von Systemdateien sinnvoll (vgl. 18.1.7 Durchführung von Sicherheitskontrollen in Client-Server-Netzen). Für diesen Zweck stellen viele Betriebssysteme bereits eigene Tools zur Verfügung.

14.5.2 Sorgfältige Durchführung von Konfigurationsänderungen

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig muss hierbei vorgegangen werden.

Insbesondere für mittlere und große Organisationen ist es unerlässlich, jede Konfigurationsänderung in einem Referenzsystem vorzubereiten und zu testen.

Bevor mit Änderungen am System begonnen wird, muss als Erstes die alte Konfiguration gesichert werden, so dass sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten.

Bei vernetzten IT-Systemen müssen die BenutzerInnen rechtzeitig über die Durchführung von Wartungsarbeiten informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Nichtverfügbarkeit des Systems einrichten und zum anderen nach Änderungen auftretende Probleme richtig zuordnen können.

Die Konfigurationsänderungen sollten immer nur schrittweise durchgeführt werden. Zwischendurch sollte immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.

Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten lässt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z. B. Boot-CD bzw. -DVD, Wiederherstellungsplatte.

Komplexere Konfigurationsänderungen sollten möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen sollten von KollegInnen überprüft werden, bevor sie in den Echtbetrieb übernommen werden.

Bei IT-Systemen mit hohen Verfügbarkeitsanforderungen ist auf Ersatzsysteme zurück zu greifen bzw. zumindest ein eingeschränkter IT-Betrieb zu gewährleisten. Das Vorgehen kann sich dabei idealerweise nach dem Disaster Recovery-Handbuch (vgl. 17 Disaster Recovery und Business Continuity) richten.

Die durchgeführten Konfigurationsänderungen sollten Schritt für Schritt notiert werden, so dass bei auftretenden Problemen das IT-System durch sukzessive Rücknahme der Änderungen wieder in einen lauffähigen Zustand gebracht werden kann.

14.6 Wartung

> *Als vorbeugende Maßnahme, um IT-Systeme vor Störungen zu bewahren, ist die ordnungsgemäße Durchführung von Wartungsarbeiten von besonderer Bedeutung.*

Dabei umfasst der Begriff Wartung

- im Falle von Hardware:
  - die Instandhaltung (vorbeugende Wartung zur Aufrechterhaltung der Betriebstüchtigkeit) und
  - die Instandsetzung (Behebung von Störungen und Fehlern zur Wiederherstellung der Betriebstüchtigkeit) durch Reparatur und Ersatz schadhafter IT-Komponenten,
- im Falle von Software:
  - die Behebung von Störungen bzw. Hilfe bei deren Umgehung und

- die Beratung der bzw. des Verantwortlichen beim Einsatz der IT-Komponenten, sowie allenfalls, abhängig von den vertraglichen Vereinbarungen,
- die Behebung von Fehlern,
- die Einrichtung und den Betrieb einer Hotline,
- die Weiterentwicklung und notwendige Anpassungen.

Richtlinien für Allgemeine Vertragsbedingungen für die Wartung von IT-Komponenten werden in den „Allgemeinen Vertragsbedingungen der Republik Österreich für IT-Leistungen“ [AVB-IT] gegeben. Dort findet sich auch eine Vorgabe für die Klassifizierung von Fehlern und die davon abgeleiteten Maßnahmen. Die AVB-IT sehen vor (siehe B Muster für Verträge, Verpflichtungserklärungen und Dokumentationen):

- Fehlerklasse 1: „kritisch“
- Fehlerklasse 2: „schwer“
- Fehlerklasse 3: „leicht“
- Fehlerklasse 4: „trivial“

14.6.1 Regelungen für Wartungsarbeiten im Haus

Für Wartungsarbeiten im Hause sind eine Reihe von Vorkehrungen und Regelungen zu treffen, von denen die wichtigsten im Folgenden zusammengefasst werden. Besonderes Augenmerk ist diesen Maßnahmen zu schenken, wenn die Arbeiten durch Externe durchgeführt werden.

- Ankündigung der Maßnahme gegenüber den betroffenen MitarbeiterInnen.
- WartungstechnikerInnen müssen sich auf Verlangen ausweisen.
- Arbeiten - insbesondere wenn sie von Externen durchgeführt werden - sind so weit zu beaufsichtigen, dass beurteilt werden kann, ob während der Arbeit nicht autorisierte Handlungen vollzogen werden und ob der Wartungsauftrag ausgeführt wurde.
- Der Zugriff auf Daten durch die WartungstechnikerInnen ist so weit wie möglich zu vermeiden. Falls erforderlich, d. h. abhängig von den Anforderungen der Informationssicherheitspolitik, sind Speichermedien evtl. vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung). Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten durch autorisierte MitarbeiterInnen genau zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen.
- Ebenfalls abhängig von den Anforderungen der Informationssicherheitspolitik muss ggf. darauf geachtet werden, ob WartungstechnikerInnen ihre eigenen mobilen IT-Geräte (Notebooks, Smartphones, Tablets, USB-Sticks etc.) in die Betriebsräume mitnehmen bzw. dort in Betrieb nehmen resp. Infrastrukturen wie WLAN oder Bluetooth benutzen dürfen. Keinesfalls sollte dies unbeaufsichtigt

geschehen. Smartphones sind mit Kameras ausgestattet, mit denen Dokumente oder Bildschirminhalte fotografiert werden können. Sie können sich auch unbemerkt über WLAN oder Bluetooth mit organisationseigenen PCs oder gar Servern verbinden.

- Die den WartungstechnikerInnen eingeräumten Zutritts- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungsarbeiten sind - je nach „Eindringtiefe“ des Wartungspersonals - Passwortänderungen erforderlich. Im PC-Bereich sollte ein Viren-Check durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Datum, betroffene IT-Komponenten, Fehlerklasse, Dauer des Ausfalls, Art und Ursache der Störung, Art der Behebung, Name des Wartungstechnikers bzw. der Wartungstechnikerin, …). Ein Muster für einen entsprechenden Störungsbericht findet sich im Anhang zu den [AVB-IT].

Folgende Regelungen sollten vertraglich festgelegt werden (vgl. dazu auch AVB-IT):

- Verpflichtung zur Geheimhaltung von Daten und Einhaltung der von der bzw. vom Verantwortlichen bekannt gegebenen Sicherheitsstandards.
- Einhaltung aller Vorschriften gemäß Datenschutzgesetz, insbesondere Verpflichtung auf §6 Datenschutzgesetz („Datengeheimnis“).
- Verpflichtung, ersetzte IT-Komponenten so zu bearbeiten, dass die auf ihnen enthaltenen Informationen nicht mehr lesbar sind, oder diese nach Vereinbarung unter Aufsicht zu zerstören. Die erfolgte Löschung oder Zerstörung ist auf Wunsch der bzw. des Verantwortlichen in jedem Einzelfall schriftlich zu bestätigen.
- Verpflichtung, Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig zu löschen.
- Festlegung der Pflichten und Kompetenzen des externen Wartungspersonals.

14.6.2 Regelungen für externe Wartungsarbeiten

Zusätzlich zu den in 14.6.1 Regelungen für Wartungsarbeiten im Haus angeführten Maßnahmen, die sinngemäß auch für die Wartung außer Haus gelten, sind eine Reihe von weiteren Maßnahmen zu treffen, die im Folgenden kurz angeführt werden.

Werden IT-Systeme zur Wartung außer Haus gegeben, sind alle vertraulichen oder geheimen Daten, die sich auf Datenträgern befinden, in Abstimmung mit der bestehenden Informationssicherheitspolitik vorher physikalisch zu löschen bzw. die Datenträger (Festplatten, aber auch z. B. Speicherkarten in Smartphones) zu

entfernen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden oder der Datenträger nicht ausgebaut werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen zu verpflichten.

Bei vergleichsweise geringwertigen Komponenten sollte ggf. überlegt werden, auf eine Reparatur zu verzichten und sie zu vernichten.

Protokollierung:
Werden Wartungsarbeiten extern durchgeführt, so sollte zusätzlich protokolliert werden:

- welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden,
- wer dies veranlasst hat,
- zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und
- wann das Gerät wieder zurückgebracht wurde.

Um dies gewährleisten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.

Weiters ist zu beachten:

- Bei Versand oder Transport der zu reparierenden IT-Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiters müssen Nachweise über den Versand (Begleitzettel, Versandscheine) und den Eingang beim Empfänger bzw. bei der Empfängerin (Empfangsbestätigung) geführt und archiviert werden.
- Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie „REPARATUR“ gesetzt werden, damit die WartungstechnikerInnen auf die Geräte zugreifen können.
- Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. *Alle* Passwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Virensuchprogramms auf Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

14.6.3 Fernwartung

Die Fernwartung von IT-Systemen birgt besondere Sicherheitsrisiken. Es ist daher sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System (einschließlich eines eventuell eingesetzten Modems) muss die folgenden Sicherheitsfunktionen realisieren:

- Bei einer Fernwartung über externe Kommunikationsverbindungen müssen die Zugänge und die Verbindungen abgesichert werden. Es muss eine Authentisierung des Fernwartungspersonals, die Verschlüsselung der übertragenen Daten und eine Protokollierung der Administrationsvorgänge gewährleistet sein. Beispielsweise kann die Anbindung per VPN oder durch exklusiv genutzte Verbindungen realisiert werden.
- Die BenutzerInnen der IT-Systeme müssen dem Fernzugriff explizit zustimmen, z. B. über eine entsprechende Bestätigung am System.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden.
- Alle Tätigkeiten bei der Durchführung der Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden, wie etwa:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte des Wartungspersonals. Das Wartungspersonal sollte nicht die vollen Administratorrechte besitzen, sondern nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.
- Auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzerkennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden.
- Wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen „Zwangslogout“ beendet werden.

Die Fernwartung sollte lokal durch IT-ExpertInnen beobachtet werden. Auch wenn die Fernwartung eingesetzt wird, weil intern das Know-how oder die Kapazität nicht verfügbar ist, kann das Wartungspersonal nicht unbeaufsichtigt gelassen werden (siehe auch 14.6.1 Regelungen für Wartungsarbeiten im Haus). Bei Unklarheiten über die Vorgänge sollte die lokale IT-Expertin bzw. der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.

Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also darf dies z. B. nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzerkennungen erfolgen.

Analog zu 14.6.2 Regelungen für externe Wartungsarbeiten sind auch für Fernwartung mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen,

- dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden,
- dass die Vorschriften über den internationalen Datenverkehr gemäß Artikel 44 ff. DSGVO (bzw. im sicherheitspolizeilichen Bereich § 58 DSG eingehalten werden,
- welche Pflichten und Kompetenzen das externe Wartungspersonal hat.

14.6.4 Wartung und administrativer Support von Sicherheitseinrichtungen

> *Viele Sicherheitsmaßnahmen erfordern zur Gewährleistung ihrer einwandfreien Funktionsfähigkeit Wartung und administrativen Support. Zu diesen Aufgaben zählen etwa die regelmäßige Auswertung und Archivierung von Protokollen, Backup, Restore und Wartung von sicherheitsrelevanten Komponenten, die Überprüfung der Parametereinstellungen und eventueller Rechte auf mögliche nicht autorisierte Änderungen, die Reinitialisierung von Startwerten oder Zählern sowie Updates der Sicherheitssoftware, wenn verfügbar (besonders, aber nicht ausschließlich, im Bereich Virenschutz) u.v.a.m.*

Alle Wartungs- und Supportaktivitäten sollten nach einem detailliert festgelegten Plan erfolgen und regelmäßig durchgeführt werden.

Die Wartung von Sicherheitseinrichtungen hat in Abstimmung mit den Verträgen, die mit den Lieferfirmen geschlossen wurden, zu erfolgen und darf nur durch dafür autorisierte Personen vorgenommen werden.

Die Kosten für Wartungs- und Supportaufgaben können im Einzelfall beträchtlich sein und sollten daher bereits bei der Auswahl der Sicherheitsmaßnahmen bekannt sein und in den Entscheidungsprozess mit einfließen.

Um die Aufrechterhaltung eines einmal erreichten Sicherheitsniveaus zu gewährleisten, ist sicherzustellen, dass

- die erforderlichen **finanziellen und personellen Ressourcen** zur Wartung von IT-Sicherheitseinrichtungen zur Verfügung stehen,
- organisatorische Regelungen existieren, die die Aufrechterhaltung der IT-Sicherheitsmaßnahmen im laufenden Betrieb ermöglichen und unterstützen,
- die Verantwortungen im laufenden Betrieb klar zugewiesen werden,

- die Maßnahmen regelmäßig daraufhin geprüft werden, ob sie wie beabsichtigt funktionieren und
- Maßnahmen verstärkt werden, falls sich neue Schwachstellen zeigen.

Alle Wartungs- und Supportaktivitäten im IT-Sicherheitsbereich sollten protokolliert werden. Der regelmäßigen Auswertung dieser Protokolle kommt besondere Bedeutung für die gesamte IT-Sicherheit zu.

14.7 Internet, Web, E-Commerce, E-Government

Aus der immer weiter verbreiteten Nutzung von E-Commerce und E-Government ergeben sich Anforderungen an die Sicherheit der Systeme, der Applikationen und der Transaktionen. Die Integrität und die Verfügbarkeit der Informationen, die von Systemen über das öffentliche Internet angeboten werden, ist sicherzustellen.

14.7.1 Richtlinien bei Verbindung mit Netzen Dritter (Extranet)

Zunehmend werden die nach außen hin abgeschotteten und abgesicherten Netzwerke von Organisationen zu einem Verbund zusammengeschlossen (Extranet). Für diesen Schritt sind als Grundlage von allen Beteiligten einzuhaltende Richtlinien bzw. Vereinbarungen notwendig.

In einer derartigen Vereinbarung (sog. Data Connection Agreement – DCA) sollen detaillierte Angaben zu folgenden Punkten enthalten sein:

- Bestimmung der Verantwortlichen
- Haftungs- und Schadensersatzregeln (z. B. auch bei Virenbefall, Hackerangriff etc.)
- eventuell Non-Disclosure-Agreement (NDA)
- Festlegung der Datennutzung
- Benennung von AnsprechpartnerInnen (in technischen, organisatorischen und sicherheitstechnischen Belangen)
- welche Dienste werden zur Verfügung gestellt (z. B. ftp, http etc.)
- welche Plattformen werden unterstützt
- Richtlinien zur Protokollierung (wer protokolliert was/wann und wie werden Protokolldaten ggf. ausgetauscht)
- welche Sicherheitsmaßnahmen müssen gewährleistet werden
- wie sind weitere Vertragspartner in die Vereinbarung einzubinden
- Regelung über das Vorgehen beim Auftreten von Sicherheitslücken (betrifft Informationspflicht, Vorgehen bei Netzwerktrennung etc.)

Sicherheitslücken müssen von allen Beteiligten vor dem Netzzusammenschluss beseitigt werden. Dabei sind gegenseitige (stichprobenartige) Überprüfungen der vereinbarten und einzuhaltenden Sicherheitsmaßnahmen sinnvoll.

14.7.2 Erstellung einer Internetsicherheitspolitik

Eine Internetsicherheitspolitik stellt eine IT-Systemsicherheitspolitik im Sinne von 4 Informationssicherheitspolitik dar. Sie muss mit der organisationsweiten Informationssicherheitspolitik der Behörde bzw. des Unternehmens kompatibel sein.

Die Erstellung der Internetsicherheitspolitik umfasst im Wesentlichen folgende Schritte (vgl. 12.1.2 Erarbeitung einer organisationsweiten Informationssicherheitspolitik):

- die Festlegung der Sicherheitsziele,
- die Auswahl der Kommunikationsanforderungen,
- die Diensteauswahl und
- organisatorische Regelungen.

Beispiele für **Sicherheitsziele** sind:

- Schutz des internen Netzes gegen unbefugten Zugriff von außen,
- Schutz einer Firewall gegen Angriffe aus dem externen Netz, aber auch gegen Manipulationen aus dem internen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,
- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit (insbesondere gilt dies auch für Informationsserver, die Informationen aus dem internen Bereich für die Allgemeinheit zur Verfügung stellen),
- Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz (Die Verfügbarkeit dieser Informationen muss aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!),
- Schutz vor Angriffen, die auf IP-Spoofing beruhen oder die Source-Routing-Option, ICMP (Internet Control Message Protocol) bzw. Routingprotokolle missbrauchen,
- Schutz vor Angriffen durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen. (Da die Anzahl der potenziellen AngreiferInnen und deren Kenntnisstand bei einer Anbindung an das Internet als sehr hoch angesehen werden muss, ist dieses Sicherheitsziel von besonderer Bedeutung.)

Im nächsten Schritt ist festzulegen, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der **Auswahl der Kommunikationsanforderungen** müssen speziell die folgenden Fragen beantwortet werden:

- Welche Informationen dürfen nach außen hindurch- bzw. nach innen hereingelassen werden?
- Welche Informationen sollen verdeckt werden (z. B. die interne Netzstruktur oder die Benutzernamen)?
- Welche Authentisierungsverfahren sollen benutzt werden (z. B. Einmalpasswörter oder Chipkarten)?
- Welche Zugänge werden benötigt (z. B. nur über einen Internetdiensteanbieter (Internet Service Provider - ISP) oder über mehrere verschiedene)?
- Welcher Datendurchsatz ist zu erwarten?

Diensteauswahl

Im dritten Schritt wird aus den Kommunikationsanforderungen abgeleitet, welche Dienste im zu sichernden Netz erlaubt und welche verboten werden müssen.

Es muss unterschieden werden zwischen denjenigen Diensten, die für die BenutzerInnen im zu schützenden Netz, und denjenigen, die für externe BenutzerInnen zugelassen werden.

In der Sicherheitspolitik muss für jeden Dienst explizit festgelegt werden,

- welche Dienste für welche BenutzerInnen oder Rechner zugelassen werden sollen und
- für welche Dienste Vertraulichkeit oder Integrität gewährleistet werden müssen.

Es sollten nur die Dienste zugelassen werden, die unbedingt notwendig sind. Alle anderen Dienste müssen verboten werden. Dies muss auch die Voreinstellung sein: Alle Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht zugelassen werden.

Die Entscheidung darüber, zu welchen Diensten BenutzerInnen im Internet Zugang erhalten kann, hängt von der Qualität der Firewall, vom dienstlichen Aufgabenbereich der BenutzerInnen sowie von ihrem Problembewusstsein ab.

Es muss festgelegt werden, ob und welche der übertragenen Nutzinformationen gefiltert bzw. überprüft werden sollen (z. B. zur Kontrolle auf Viren).

Die Sicherheitspolitik sollte so beschaffen sein, dass sie auch zukünftigen Anforderungen gerecht wird, d. h. es sollte eine ausreichende Anzahl von Verbindungsmöglichkeiten vorgesehen werden. Jede spätere Änderung muss streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

Ausnahmeregelungen, insbesondere für neue Dienste und kurzzeitige Änderungen (z. B. für Tests), müssen vorgesehen werden.

Darüber hinaus sind eine Reihe von **organisatorischen Regelungen** erforderlich, wie beispielsweise:

- Es müssen Verantwortliche sowohl für die Erstellung als auch für die Umsetzung und die Kontrolle der Einhaltung der Internetsicherheitspolitik benannt werden (z. B. Informationssicherheitskoordinatoren im Bereich, siehe 6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit).
- Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.
- Die BenutzerInnen müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung, umfassend informiert werden.
- Jeder Internetdienst birgt Gefahren, die nicht auf technischer Ebene durch eine Firewall abgefangen werden können. Es ist daher eine Schulung erforderlich, die den BenutzerInnen mögliche Risiken aufzeigt und ihr Problembewusstsein fördert.
- Angriffe auf eine Firewall sollten nicht nur erfolgreich verhindert, sondern auch frühzeitig erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Die Firewall sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z. B. häufigen fehlerhaften Passworteingaben auf einem Application-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.
- Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z. B. die AngreiferInnen verfolgt werden sollen oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt, und die entsprechenden Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.
- Daneben müssen je nach Organisationsstruktur und -größe ein oder mehrere Verantwortliche für die Pflege der angebotenen Kommunikationsdienste benannt werden. Neben dem Serverbetrieb wie E-Mail-, oder Web-Server müssen auch die von den BenutzerInnen eingesetzten Kommunikationsclients betreut werden.

14.7.3 Festlegung einer WWW-Sicherheitsstrategie

Vor der Nutzung von WWW-Diensten (World Wide Web) ist zunächst in einem Konzept darzustellen, welche Dienste genutzt und welche angeboten werden sollen. Hierbei ist die Absicherung eines Webservers ebenso zu betrachten wie die der Webclients und der Kommunikationsverbindungen zwischen diesen.

Webserver sind für HackerInnen sehr attraktive Ziele, da einem erfolgreichen Angriff oft sehr große Publizität zuteil wird. Daher muss der Absicherung eines Webservers ein hoher Stellenwert eingeräumt werden. Vor dem Einrichten eines Webservers sollte in einer WWW-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der WWW-Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind.

In der WWW-Sicherheitsstrategie muss neben einer Sicherheitsstrategie für den Betrieb eines Webservers auch eine Sicherheitsstrategie für die WWW-Nutzung enthalten sein.

WWW-Sicherheitsstrategie für den Betrieb eines Webservers

In der Sicherheitsstrategie für den Betrieb eines Webservers sollten die folgenden Fragen beantwortet werden:

- Wer darf welche Informationen einstellen?
- Welche Randbedingungen sind beim Betrieb eines Webservers zu beachten?
- Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen?
- Welche Dateien dürfen aufgrund ihres Inhaltes nicht auf dem Webserver eingestellt werden (z. B. weil die Inhalte vertraulich sind, nicht zur Veröffentlichung zulässig sind oder nicht der Firmen- bzw. Behördenpolitik entsprechen)?
- Welche Zugriffsbeschränkungen auf den Webserver sollen realisiert werden?

Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potenzielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. Eine wichtige Informationsquelle für Sicherheitshinweise zur WWW-Nutzung stellt die „World Wide Web Security FAQ“ (unter http://www.w3.org/Security/Faq/) und das „Open Web Application Security Project“ (unter https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) dar.

WWW-Sicherheitsstrategie für die WWW-Nutzung

In der Sicherheitsstrategie für die WWW-Nutzung sollten die folgenden Fragen beantwortet werden:

- Wer erhält WWW-Zugang?
- Welche Randbedingungen sind bei der WWW-Nutzung zu beachten?
- Wie werden die BenutzerInnen geschult?
- Wie wird technische Hilfestellung für die BenutzerInnen gewährleistet?

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere folgende Punkte zu gewährleisten:

- Die Browser der BenutzerInnen müssen durch die AdministratorInnen so vorkonfiguriert sein, dass ohne weiteres Zutun der BenutzerInnen maximale Sicherheit erreicht werden kann (siehe auch 14.7.5 Sicherheit von Webbrowsern).
- Dateien, deren Inhalt Anstoß erregen könnte, dürfen weder auf Webservern eingestellt noch nachgefragt werden. Es muss festgelegt werden, welche Inhalte als anstößig gelten.
- Nach dem Download von Dateien sind diese explizit auf Viren zu überprüfen, soweit dies nicht durch eine zentrale Überprüfung gewährleistet wird.

Alle Regelungen und Bedienungshinweise zur WWW-Nutzung sind schriftlich zu fixieren und sollten den MitarbeiterInnen jederzeit zur Verfügung stehen.

Die BenutzerInnen müssen vor der WWW-Nutzung geschult werden, sowohl in der Nutzung ihrer Webbrowser als auch des Internets, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden.

14.7.4 Sicherer Betrieb eines Webservers

> *Webserver sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Das Betriebssystem und die Software müssen so konfiguriert sein, dass der Rechner optimal gegen Angriffe geschützt wird. Solange der Rechner nicht entsprechend konfiguriert ist, darf er nicht ans Netz genommen werden.*

Daher sollte ein Webserver, der Informationen im Internet anbietet, entsprechend den folgenden Vorgaben installiert werden:

- Auf einem Webserver sollte nur ein Minimum an Programmen vorhanden sein, d. h. das Betriebssystem sollte auf die unbedingt erforderlichen Funktionalitäten reduziert werden und auch sonst sollten sich nur unbedingt benötigte Programme auf dem Webserver befinden.
- Ein Webserver sollte insbesondere keine unnötigen Netzdienste enthalten, verschiedene Dienste gehören auf verschiedene Rechner (beispielsweise ein Webserver und ein E-Mail-Server).
- Der Zugriff auf Dateien oder Verzeichnisse muss geschützt werden (siehe 14.7.6 Schutz der WWW-Dateien).
- Die Kommunikation mit dem Webserver sollte durch einen Paketfilter auf ein Minimum beschränkt werden.
- Die Administration des Webserver sollte nur über eine sichere Verbindung erfolgen, d. h. die Administration sollte direkt an der Konsole, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.

- Weiters sollte der Webserver vor dem Internet durch einen Firewall-Proxy oder aber zumindest durch einen Paketfilter abgesichert werden. Er darf sich nicht zwischen Firewall und internem Netz befinden, da ein Fehler auf dem Webserver sonst Zugriffe auf interne Daten ermöglichen könnte.

Je nach Art des Webservers bieten sich unterschiedliche Möglichkeiten zum Schutz an. Allen diesen Möglichkeiten gemeinsam ist allerdings, dass der eigentliche Serverprozess des Webservers, nämlich der HTTP-Daemon, nur mit eingeschränkten Rechten ausgestattet sein sollte. Er muss üblicherweise mit root-Privilegien gestartet werden, sollte aber nach dem Start so schnell wie möglich mit den Rechten eines weniger privilegierten neuen Benutzers weiterarbeiten. Hierfür sollte ein eigener Benutzeraccount wie *wwwserver* eingerichtet werden. Wichtig ist, dass dieser Account keine Schreibrechte auf die Protokolldateien besitzt. AngreiferInnen könnten sonst durch Ausnutzung eines Fehlers diese mit den Rechten des HTTP-Servers manipulieren.

Für die verschiedensten Server-Produkte sind teilweise detaillierte Leitlinien zu deren sicheren Konfiguration verfügbar.

14.7.5 Sicherheit von Webbrowsern

Beim Zugriff auf das World Wide Web (WWW) können verschiedene Sicherheitsprobleme auf den angeschlossenen Arbeitsplatzrechnern auftreten.

Ursachen dafür können sein:

- falsche Handhabung durch die BenutzerInnen
- unzureichende Konfiguration der benutzten Browser
- Sicherheitslücken in den Browsern.

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen werden und ohne Nachfrage auf dem lokalen Rechner ausgeführt werden (z. B. JavaScript o.ä., vgl. 13.1.16 Firewalls und aktive Inhalte). Auch innerhalb von Dokumenten oder Bildern können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können (z. B. Makroviren in Word- oder Excel-Dokumenten). Um solche Probleme zu vermeiden, sollten die im Folgenden beschriebenen Maßnahmen umgesetzt werden. Darüber hinaus kann es auch sinnvoll sein, produktspezifische Konfigurationsleitlinien zu verwenden.

Laden von Dateien oder Programmen:

Beim Laden von Dateien oder Programmen können eine Vielzahl von Sicherheitsproblemen auftreten, die bekanntesten sind sicherlich Schadprogramme wie Viren, Makroviren und „Trojanische Pferde“. Die BenutzerInnen dürfen sich nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen.

Bei der Konfiguration des Browsers ist darauf zu achten, dass bei Dateitypen, die Makroviren enthalten können, die zugehörigen Anwendungen nicht automatisch gestartet werden.

Aktuelle Virenschutzprogramme sollten auf *allen* Rechnern mit Internetzugang installiert sein und automatisch ausgeführt werden.

Alle BenutzerInnen müssen darauf hingewiesen werden, dass sie selbst dafür verantwortlich sind, beim Dateiladen alle entsprechenden Vorsichtsmaßnahmen zu ergreifen. Selbst wenn über die Firewall automatisch die geladenen Informationen auf Viren überprüft werden, bleiben die BenutzerInnen verantwortlich für die Schadensfreiheit von geladenen Dateien oder Programmen. Grundsätzlich müssen bei der Installation von Programmen natürlich die organisationsinternen Sicherheitsregeln beachtet werden. Insbesondere dürfen nur getestete und zugelassene Programme installiert werden (vgl. dazu auch 14.1.7 Abnahme und Freigabe von Software, 14.1.8 Installation und Konfiguration von Software und 14.3.1 Nutzungsverbot nicht freigegebener Software). Vor der Installation sollten auf Stand-alone-Rechnern Tests auf die Schadensfreiheit der Programme durchgeführt werden. In Zweifelsfällen ist die IT-Administration hinzuzuziehen.

Werbeblocker-Erweiterungen (Ad-Blocker) für den Browser tragen teilweise auch zum Schutz vor Schadprogrammen bei, indem bekannte schädliche Domains blockiert werden und ein Aufruf bzw. Download somit nicht mehr möglich ist. Außerdem sind eingebettete Werbeanzeigen und Drittinhalte oft Einfallstor für Schadprogramme oder Weiterleitungen auf betrügerische Webseiten. Mit aktivem Ad-Blocker werden solche Inhalte und die dabei integrierten Skripte gar nicht erst aufgerufen bzw. geladen und ausgeführt.

Plug-Ins, Zusatzprogramme und Erweiterungen

Nicht alle Browser können alle Dateiformate direkt verarbeiten, d. h. i. Allg. anzeigen, in manchen Fällen auch abspielen. Bei einigen Dateiformaten werden zusätzlich noch Plug-Ins bzw. Zusatzprogramme benötigt.

Bei Plug-Ins handelt es sich um Bibliotheksdateien (z. B. DLL-Dateien), die von Installationsprogrammen ins Plug-In-Verzeichnis geladen werden und bei Aufruf des entsprechenden Dateiformates vom Browser ausgeführt werden (z. B. H.264 Video-Decoder oder ehemals Flash-Plug-In).

Zusatzprogramme, z. B. Viewer, sind eigenständige Programme, die in der Lage sind, bestimmte Dateiformate zu verarbeiten. Der Aufruf eines solchen Zusatzprogramms wird über eine Konfigurationsdatei des Browsers gesteuert, in der Dateiendung und Programm verknüpft sind. Bei Viewern von Office-Dokumenten sollte darauf geachtet werden, dass diese keine Makrobefehle ausführen können (Schutz vor Makroviren, vgl. 12.3.6 Vermeidung bzw. Erkennung von Viren durch die BenutzerInnen).

Die meisten Browser bieten außerdem noch die Möglichkeit individuelle Erweiterungen (auch als Add-Ons bezeichnet) zu installieren. Mit Hilfe dieser sind verschiedenste Änderungen an der Verarbeitung und Aufbereitung der aufgerufenen Webseiten, aber auch am Browser selbst, möglich.

Beim Hinzufügen von Plug-Ins, Zusatzprogrammen bzw. Erweiterungen für einen Webbrowser sind dieselben Vorsichtsmaßnahmen wie beim Laden von Dateien oder Programmen zu beachten. Es dürfen keine Programme installiert werden, denen man nicht unbedingt vertrauen kann.

Solche Zusatzkomponenten verlängern die Startzeit des Browsers und erhöhen das Risiko potenzieller Schwachstellen. Daher sollten alle nicht benötigten Plug-Ins und Erweiterungen entfernt werden.

Cookies

In sogenannten Cookie-Dateien werden auf dem Rechner der BenutzerInnen Informationen über abgerufene Webseiten, Sitzungen (Sessions) und Benutzerverhalten gespeichert. Damit können Webseiten beim nächsten Besuch der jeweiligen BenutzerInnen spezielle Informationen für diese anbieten oder diesen bestimmte Dienste zugänglich machen. Allerdings können Webseiten hiermit auch Benutzerprofile erstellen, z. B. für zielgruppenorientierte Werbung.

Um dies zu verhindern, sollte das Anlegen von Cookie-Dateien verhindert bzw. abgelehnt werden oder, wo das nicht möglich ist, diese regelmäßig gelöscht werden. Grundsätzlich müssen Webseiten im Anwendungsbereich der DSGVO die Ablehnung nicht notwendiger Cookies ermöglichen. Hierauf kann man sich jedoch nicht ganz verlassen und auch bei der Deklaration der notwendigen Cookies wird vielfach Interpretationsspielraum ausgenützt. Cookies finden sich meist im Konfigurationsverzeichnis des benutzten Webbrowsers in Dateien wie *cookies.sqlite* oder Verzeichnissen wie *cookies*, sind aber auch direkt im Browser über die Adressleiste oder die Konsole bzw. Entwickleroptionen einsehbar.

Um das Anlegen von Cookie-Dateien zu verhindern, kann auch eine leere Cookie-Datei angelegt werden und mit einem Schreibschutz versehen werden. Inwieweit dies effektiv ist, hängt vom eingesetzten Betriebssystem und der Browser-Variante ab. Hier ist insbesondere zu überprüfen, ob der Browser weder den Schreibschutz zurücksetzen kann noch dadurch einen Absturz verursacht.

Eine weitere Möglichkeit zum Blockieren von Cookies ist die Verwendung von Browser-Erweiterungen, z. B. Ad-Blocker oder Privacy-Add-Ons. Je nach Erweiterung können diese Cookies generell blockieren oder das Auslesen durch Dritte verhindern.

Normalerweise bieten Browser in den Einstellungen die Möglichkeit alle Cookies zu löschen, sobald der Browser geschlossen wird. Ansonsten kann es hilfreich sein, das regelmäßige Löschen der Cookies über eine Batch-Datei zu steuern, die beispielsweise bei jedem Systemstart oder jeder Benutzeranmeldung die alten Cookie-Dateien löscht.

Datensammlungen

Nicht nur extern werden Daten über die Internetnutzung der verschiedenen BenutzerInnen gesammelt, sondern auch lokal. Auch hier muss sichergestellt werden, dass nur Befugte darauf Zugriff haben können. Dies gilt insbesondere auch für die von Browsern angelegten Dateien über History, Hotlists und Cache. Die BenutzerInnen müssen informiert werden, wo auf ihren lokalen Rechnern solche Daten gespeichert werden und wie sie diese löschen können.

Diese Dateien sind auf Proxy-Servern besonders sensibel, da auf einem Proxy-Server alle externen WWW-Zugriffe aller MitarbeiterInnen protokolliert werden, inklusive der IP-Adresse des Clients, der die Anfrage gestartet hat, und der nachgefragten URL. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutz-Verletzungen nach sich ziehen.

Von den meisten Browsern werden viele Informationen über die BenutzerInnen und ihr Nutzerverhalten gesammelt, von denen diese einerseits vielleicht nicht wollen, dass sie weitergegeben werden, und die anderseits in ihrer Masse den verfügbaren Speicherplatz mit überflüssigen Informationen blockieren. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene Webseiten,
- History-Datenbank (s. u.),
- URL-Liste (Liste der letzten aufgerufenen URLs),
- Cookie Liste,
- Informationen über BenutzerInnen, die im Browser gespeichert und evtl. auch weitergegeben werden (s. u.),
- Informationen im Cache (s. u.).

History-Datenbank

History-Datenbanken enthalten eine vollständige Sammlung über alle Aktivitäten, die mit einem Browser durchgeführt worden sind, d. h. Angaben über betrachtete Bilder, Adressen, evtl. betrachtete vertrauliche interne Dokumente etc. Daher sollte die Datenbank regelmäßig aufgeräumt werden.

Informationen über BenutzerInnen

In einem Browser und den darin aufgerufenen Webseiten werden auch diverse Informationen über BenutzerInnen gespeichert und evtl. auch weitergegeben, z. B. Realname, E-Mail-Adresse, Organisation. Um nicht mit Werbe-E-Mail überflutet zu werden oder Opfer eines Identitätsdiebstahls oder CEO-Betrugs zu werden, empfiehlt es sich, für die Browser-Benutzung einen Alias zu verwenden und Echt-Daten nur soweit unbedingt nötig und nur auf vertrauenswürdigen Webseiten anzugeben.

Informationen im Cache

*Viele Browser erzeugen in einem Cache-Verzeichnis große Mengen an Dateien, die den Text und die Bilder aller besichtigten Web-Seiten enthalten, seit der Cache das letzte Mal gelöscht wurde. Der Cache dient dazu das mehrfache Laden von Informationen einer Seite während **einer** Sitzung zu verhindern. Manche Browser löschen diese Daten, die in jeder weiteren Sitzung oft nutzlos sind, allerdings nicht eigenständig, so dass sich in einem nicht regelmäßig gelöschten Cache schnell Dutzende Megabyte Datenmüll ansammeln. Aus diesen Daten lassen sich darüber hinaus auch Benutzerprofile erstellen. Daher sollte der Cache ebenso wie der Verlauf regelmäßig gelöscht werden.*

Wenn auf mit TLS gesicherte WWW-Seiten zugegriffen wird, kann dies unter anderem dazu dienen, sensible Informationen wie Kreditkartennummern verschlüsselt über das Internet zu übertragen. Daher sollten solche Seiten von vornherein nicht im Cache abgelegt werden.

Zugriff auf Client-Festplatte

Bei einigen Browsern wird Webservern die Möglichkeit gegeben, aktiv auf die Festplatte des Clients zuzugreifen.

Diese – bis auf JavaScript - mittlerweile veralteten und nichtmehr recht gebräuchlichen Technologien (ActiveX, Java, Flash, Silverlight) werden beispielsweise über den Browser statt auf dem Server auf der Client-Seite ausgeführt. Dies führt aber zu einer Verlagerung des Sicherheitsrisikos vom Server

auf den Client. Daher sind zwar verschiedene Sicherheitsmechanismen eingebaut, um einen möglichen Missbrauch zu verhindern, allerdings sind bereits mehrfach Sicherheitslücken gefunden worden. Bis auf JavaScript werden diese Technologien von aktuellen Browsern auch nicht mehr unterstützt bzw. werden blockiert.

Die Benutzung von Browsern, die Zugriffe auf Dateien des Client gestatten, birgt in diesem Zusammenhang gewisse Sicherheitsrisiken. ActiveX erlaubt unter bestimmten Bedingungen die Nutzung lokaler Ressourcen. Bei Java ist ein solcher Zugriff ebenfalls möglich, jedoch nur wenn die AnwenderInnen dies explizit gestatten. Das Sicherheitskonzept von ActiveX basiert darauf, dass die AnwenderInnen dem Anbieter und einer authentifizierten dritten Stelle im World Wide Web vertraut. Dieses Vertrauen ist problematisch, wenn Web-Seiten eines unbekannten oder eines neuen Anbieters aufgerufen werden.

Aufgrund der bestehenden Probleme mit ActiveX, Java und JavaScript sollten diese generell abgeschaltet werden. Falls die Benutzung von ActiveX, Java und JavaScript unbedingt notwendig ist, sollten diese nur auf Rechnern zugelassen sein, die gegenüber anderen internen Rechnern so abgeschottet sind, dass die Vertraulichkeit und Integrität sicherheitsrelevanter Daten nicht beeinträchtigt werden können.

Sicherheitslücken in den Webbrowsern

In den meisten Browsern sind bereits gravierende Sicherheitslücken gefunden worden. Es ist daher sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren und entsprechende Gegenmaßnahmen zu ergreifen.

Mögliche Gegenmaßnahmen sind das Einspielen von Patches zur Beseitigung bekannter Sicherheitslücken, der Einsatz neuer Versionen (Achtung: gerade in neuen Versionen können evtl. neue, zunächst noch unbekannte Sicherheitsprobleme auftreten!), sowie zusätzliche organisatorische und administrative Maßnahmen. Nicht mehr unterstützte Browser, wie zum Beispiel der Microsoft Internet Explorer, oder schlecht gewartete Browser sollten auf keinen Fall verwendet werden.

Verschlüsselung

Da im Internet Daten auch im Klartext übertragen werden, sollten sensible Daten nur verschlüsselt übertragen werden. Hierbei wäre es sinnvoll, wenn entsprechende Mechanismen schon in den unteren Schichten des Protokolls vorgesehen würden. Es ist zu überlegen, welche Protokolle (z.B. IPsec, HTTPS bzw. TLS oder DTLS) hierfür eingesetzt werden sollen.

Nutzung vorhandener Sicherheitsfunktionalitäten

Die vorhandenen Sicherheitsfunktionalitäten der Browser (Rückfrage vor dem Ausführen von Programmen, Zugriff nur auf eingeschränkte Dateisysteme, keine Möglichkeit zum Verändern lokaler Daten) sollten auf jeden Fall genutzt werden.

Beim Surfen im Internet sollte die automatische Ausführung von Programmen verhindert werden und nur bei vertrauenswürdigen Servern wieder eingeschaltet werden.

E-Mail-Clients bieten häufig die Möglichkeit, beliebige Daten im MIME-Format (Multipurpose Internet Mail Extensions) zu lesen. Auch in diesen Daten können Befehle enthalten sein, die zu einem automatischen Starten von Programmen auf dem lokalen Rechner führen. Die entsprechenden Möglichkeiten sollten daher in der Konfiguration deaktiviert werden bzw. nur nach Rückfrage gestartet werden können.

Regelungen

Ein Großteil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der BenutzerInnen, da deren Umsetzung wie beispielsweise die Aktivierung bestimmter Optionen nicht ständig durch die Systemadministration überprüft werden kann. Daher sollten alle BenutzerInnen vor der Nutzung von Internetdiensten durch entsprechende Anweisungen verpflichtet werden, die aufgeführten Sicherheitsrichtlinien zu beachten. Es empfiehlt sich vor der Zulassung von BenutzerInnen zu Internetdiensten, diese auf eine Benutzungsordnung zu verpflichten. Die Inhalte der Internetsicherheitsrichtlinie und der Benutzungsordnung sind den BenutzerInnen in einer Schulung darzulegen.

In dieser Benutzungsordnung sollten die zur Verfügung stehenden Kommunikationsdienste kurz erläutert und alle relevanten Regelungen aufgeführt werden. Alle BenutzerInnen sollten durch Unterschrift bestätigen, dass die dargestellten Regelungen zur Kenntnis genommen wurden und bei Benutzung der Kommunikationsdienste beachtet werden.

Weiters müssen die BenutzerInnen darauf hingewiesen werden,

- dass die Konfiguration der WWW-Programme nicht eigenmächtig geändert werden darf,
- welche Daten protokolliert werden,
- wer die Ansprechpartner bei Sicherheitsproblemen sind.

14.7.6 Schutz der WWW-Dateien

Die Dateien und Verzeichnisse auf einem Webserver müssen gegen unbefugte Veränderungen, aber auch u.U. - abhängig von den Sicherheitsanforderungen - gegen unbefugten Zugriff geschützt werden. Generell muss zwischen zwei verschiedenen Aspekten unterschieden werden, nämlich dem Schutz vor unbefugtem Zugriff lokaler BenutzerInnen und dem Schutz vor unbefugtem Zugriff von außen über das Web.

Generelle Aspekte

Falls das Webangebot nicht nur aus statischen HTML-Dateien besteht, sondern bestimmte Inhalte dynamisch erzeugt werden, so müssen die dazu benutzten Programme (beispielsweise PHP-Skripte, Java Server Faces) besonders sorgfältig programmiert werden, um zu verhindern, dass auf diesem Weg ein unbefugter Zugriff oder gar eine Kompromittierung des Servers erfolgen kann.

Eine Möglichkeit, unbefugten Zugang zu erschweren, ist es, die Scripts unter einer Benutzer-ID auszuführen, die nur Zugang zu ausgewählten Dateien hat. Insbesondere ist es wichtig, die Konfigurationsdateien zu schützen, da sonst alle Zugangsrestriktionen leicht ausgeschaltet werden können.

Die Schreib- und Leserechte der WWW-Dateien sollten als lokale Dateien nur berechtigten BenutzerInnen Zugang erlauben.

Schutz vor unbefugten Veränderungen

Auf einem typischen Webserver ändern sich nur die Protokolldateien ständig, alle anderen Dateien sind statisch. Dies trifft insbesondere auf Systemprogramme und die WWW-Seiten zu. WWW-Seiten werden zwar regelmäßig aktualisiert, sollten aber nicht auf dem Webserver selbst bearbeitet werden.

Um sicherzustellen, dass keine Dateien auf dem Webserver unbemerkt abgeändert werden können, sollten über alle statischen Dateien und Verzeichnisse Prüfsummen gebildet und regelmäßig überprüft werden. Um zu verhindern, dass WWW-Dateien überhaupt von Unbefugten geändert werden können, können statische Daten auf einem schreibgeschützten Speichermedium (z. B. DVD-ROM oder Festplatte mit Schreibschutz) gespeichert werden.

Schutz vor unbefugtem Zugriff

Der Zugriff auf Dateien oder Verzeichnisse eines Webservers ist zu schützen.

Diese können auf verschiedene Arten geschützt werden:

- Der Zugriff kann auf frei wählbare IP-Adressen, Teilnetze oder Domänen beschränkt werden.
- Es können benutzerspezifische Kennungen und Passwörter vergeben werden.

- Zugriffskontrolle wäre auch durch eine TLS-Verbindung mit clientseitigen Zertifikaten zur Authentifizierung möglich. Generelles zu Zertifikaten in der öffentlichen Verwaltung siehe [IKTB-110903-3] und [IKTB-281003-19] .
- Die Dateien können verschlüsselt abgelegt werden und die zugehörigen kryptographischen Schlüssel werden nur dem Zielpublikum bekannt gegeben.

14.7.7 Einsatz von Stand-alone-Systemen zur Nutzung des Internets

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN entstehen, zu verringern, ist es sinnvoll Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu einem LAN haben.

Hierfür bieten die verschiedenen Betriebssysteme unterschiedliche Möglichkeiten mit jeweils spezifischen Gefährdungen für die Vertraulichkeit und Integrität der Daten auf diesem Rechner.

Wichtig ist es zu beachten, dass bei der Installation der Internetzugangssoftware keine unnötigen Programme installiert werden. So gibt es bei einigen Produkten und Betriebssystemen die Möglichkeiten, durch die Installation von Server-Programmen den Rechner zu einem vollständigen Internetserver zu machen. Die Installation der TCP/IP-Software bietet eine vollständige bidirektionale Verbindung zum Internet, über die Daten sowohl ins Internet geschickt als auch von dort abgeholt werden können.

14.7.8 Sichere Nutzung von E-Commerce- bzw. E-Government-Applikationen

E-Commerce- und E-Government-Anwendungen ergänzen zunehmend das Angebot im Internet. Beispielhafte Applikationen in diesem Sinne wären Online-Banking, Internet-Shopping oder das Angebot von Behörden wie etwa FinanzOnline. Bei diesen Anwendungen sollte in der Regel ein hohes Maß an Sicherheit gewahrt werden.

Über generelle Empfehlungen hinaus (vgl. 14.7.5 Sicherheit von Webbrowsern), sind auch die folgenden Empfehlungen und Kriterien in diesem Zusammenhang zu beachten:

- Die Anwendung muss die Anforderungen an Datenschutz und Datensicherheit erfüllen. Einschlägigen Richtlinien und Normen (z. B. ÖNORM A7700 „Sicherheitstechnische Anforderungen an Webapplikationen“) sind zu berücksichtigen.

- Bei Anwendungen mit sehr hohem Schutzbedarf soll die Erfüllung dieser Anforderungen durch unabhängige Dritte (z. B. externe Audits, Zertifizierung nach ÖNORM A7700) überprüft werden.
- Clientseitig sind Virenschutzmaßnahmen zu treffen (vgl. 12.3 Schutz vor Schadprogrammen und Schadfunktionen).
- Im Falle notwendiger spezieller Software (z. B.: Online-Banking-Software) ist diese nur von vertrauenswürdigen Quellen zu beziehen und es ist auf dessen Aktualität (bzgl. Updates, sicherheitsrelevanter Patches etc.) zu achten.
- Die für derartige Internetanwendungen genutzten Rechner sollten festen BenutzerInnen zugeordnet sein – öffentlich zugängliche Internet-PCs sollten dafür nicht herangezogen werden.
- Die Verwendung von mittels TLS verschlüsselten Verbindungen ist bei E-Commerce- und E-Government-Anwendungen immer vorauszusetzen (vgl. 14.7.5 Sicherheit von Webbrowsern). Zu diesem Thema veröffentlicht die „Operative Unit“ des „Chief Information Office“ ein Papier zur Kategorisierung von TLS-Verbindungen.
- Werden TLS-Zertifikate zur Authentisierung des Servers verwendet, so ist auf deren Gültigkeit sowie auf die Übereinstimmungen zwischen Server und den Angaben im Zertifikat zu achten.
- Bei E-Government-Anwendungen ist beim Serverzertifikat auf die Verwaltungseigenschaft (vgl. die „Richtlinien für Zertifikate für das E-Government (E-Government OID)“ [IKT-ZERT]) und auf eine geeignete Zertifikatshierarchie zu achten [IKTB-110504-02] .
- Um dem Missbrauch reservierter Domänen in abgewandelter Form vorzubeugen, wird empfohlen für Domänen mit Umlauten, diese in beiden Schreibweisen (z. B. sowohl „ae“ als auch „ä“) einzurichten [IKTB-110504-01] .
- Zur Verringerung der Länge der Signaturstrings ist die Verwendung von elliptischen Kurven anzuraten. Die MOA-Dienste sind für diese Kurven vorbereitet [IKTB-110505-03] .
- Für elektronische Bescheide wird das Bescheidschema empfohlen [IKTB-230904-01] .

14.7.9 Portalverbundsystem in der öffentlichen Verwaltung

Bezug: Österreich

Der Portalverbund ist ein Zusammenschluss von Verwaltungsportalen zur gemeinsamen Nutzung der bestehenden Infrastruktur. Der Vorteil eines Portals ist, dass mehrere Anwendungen über einen Punkt zugänglich sind.

Portale zwischen den Verwaltungen bilden die technische Basis für das zentrale Melderegister, für EKIS, das Elektronische Kriminalpolizeiliche Informationssystem, und für eine Reihe weiterer wichtiger Anwendungen verschiedener Ressorts.
Im Portalverbund wird durch - mit einheitlichen Attributen versehene - Zertifikate einerseits die Sicherheit aber andererseits auch die Offenheit gegenüber dem Markt erreicht.

Seitens der Arbeitsgruppe (Bund / Länder) wurde ein Protokoll (Spezifikation Portal Verbund Protokoll PVP [IKT-PVP]) und eine Struktur (Spezifikation LDAP-gv.at [IKT-LDAP]) zum Portalverbund vorgeschlagen. Diese wurde im Rahmen des IKT-Board-Beschlüsse [IKTB-040402-3] und [IKTB-051102-1] zur Verwendung in der öffentlichen Verwaltung empfohlen. Seitens des IKT-Boards werden zusätzliche Anmerkungen zur Verständlichkeit angefügt:

- Soweit symmetrische Schlüssel angewendet werden, sind die Schlüssellängen mit mindestens 100 Bit zu wählen.
- Für die Zertifikate von Server und Client sind Zertifizierungsdienste zu verwenden, deren Sicherheitsvorgaben nach österreichischer Rechtslage wirksam sind.
- Generell haben sich Portale, die an andere Portale koppeln, dies mit Client-Identifikation via Zertifikat durchzuführen.
- Diese Portalstruktur ist für Organwalter und gesetzliche Vertretungen für den jeweils eigenen Wirkungsbereich - nicht jedoch für BürgerInnen anwendbar.
- Bei der Umsetzung von Anwendungsportalen ist darauf zu achten, dass diese das Portalverbundprotokoll unterstützen. Die BenutzerInnen sind dabei entsprechend der Organisationszugehörigkeit zu erfassen [IKTB-240304-01] .
- Bei Zugriff auf Verwaltungsanwendungen (z. B. ESS/SAP - SAP Employee Self Service) ist auf die entsprechende Sicherheitsklasse des Zugangs zu achten [IKTB-270705-01] .
- Weitere Portalkopplungsstrukturen werden nur nach vorheriger Abstimmung zwischen Bund, Ländern, Städten und Gemeinden eingesetzt.

Für die Signatur und die Identifikation wird empfohlen die Module für Sicherheitstechniken für Online-Verfahren (MOA-ID, MOA-SS/SP) einzubinden [IKTB-161203-01] . Im Rahmen der Anwendungen des Bundes werden diese dann auch zur Sicherung der Konvergenz verwendet. Neben den Protokollen für den Portalverbund ist eine einheitliche Vorgehensweise in den Bereichen

- verwendbare Verschlüsselungsverfahren,
- Zertifikatsspezifikationen,
- Keystoreformate und
- Zertifikatsmanagement

anzuwenden.

In Hinblick auf die Verwendung von Zertifikaten in der öffentlichen Verwaltung werden besonders in den IKT-Board-Beschlüssen [IKTB-110903-3] und [IKTB-281003-19] entsprechende Dokumente und Richtlinien beschlossen und zur Anwendung empfohlen (siehe dazu auch Richtlinien der IKT-Stabsstelle für Serverzertifikate [IKT-SZERT]).

15 Lieferantenbeziehungen

15.1 Dienstleistungen durch Dritte (Outsourcing)

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen. Dabei ist es unerheblich, ob die Leistung in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht wird. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes.

Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird: *Tasksourcing* bezeichnet das Auslagern von Teilbereichen. Werden Dienstleistungen mit Bezug zur IT-Sicherheit ausgelagert, wird von *Security Outsourcing* oder *Managed Security Services* gesprochen. Beispiele sind die Auslagerung des Firewall-Betriebs, die Überwachung des Netzes, Virenschutz oder der Betrieb eines Virtual Private Networks (VPN). Unter *Application Service Provider (ASP)* versteht man einen Dienstleister, der auf seinen eigenen Systemen einzelne Anwendungen oder Software für seine Kunden betreibt (E-Mail, SAP-Anwendungen, Archivierung, Web-Shops, Beschaffung). Auftraggeber und Dienstleister sind dabei über das Internet oder ein VPN miteinander verbunden. Beim *Application Hosting* ist ebenfalls der Betrieb von Anwendungen an einen Dienstleister ausgelagert, jedoch gehören im Gegensatz zum ASP-Modell die Anwendungen noch dem jeweiligen Kunden. Da die Grenzen zwischen klassischem Outsourcing und reinem ASP in der Praxis zunehmend verschwimmen, wird im Folgenden nur noch der Oberbegriff Outsourcing verwendet. Das Auslagern von Geschäfts- und Produktionsprozessen ist ein etablierter Bestandteil heutiger Organisationsstrategien. Speziell in den letzten beiden Jahrzehnten hat sich der Trend zum Outsourcing enorm verstärkt, und dieser scheint auch für die nächste Zukunft ungebrochen. Es gibt aber inzwischen auch publizierte Beispiele für gescheiterte Outsourcing-Projekte, wo der Auftraggeber den Outsourcing-Vertrag gekündigt hat und die ausgelagerten Geschäftsprozesse wieder in Eigenregie betreibt (Insourcing). Die Gründe für Outsourcing sind vielfältig: die Konzentration einer Organisation auf ihre Kernkompetenzen, die Möglichkeit einer Kostenersparnis (z. B. keine Anschaffungs- oder Betriebskosten für IT-Systeme), der Zugriff auf spezialisierte Kenntnisse und Ressourcen, die Freisetzung interner Ressourcen für andere Aufgaben, die Straffung der internen Verwaltung, die verbesserte Skalierbarkeit der Geschäfts- und Produktionsprozesse, die Erhöhung der Flexibilität sowie der Wettbewerbsfähigkeit einer Organisation sind nur einige Beispiele. Beim Auslagern von IT-gestützten Organisationsprozessen werden die IT-Systeme und Netze der auslagernden Organisation und ihres Outsourcing-Dienstleisters in der Regel eng miteinander

verbunden, so dass Teile von internen Geschäftsprozessen unter Leitung und Kontrolle eines externen Dienstleisters ablaufen. Ebenso findet auf personeller Ebene ein intensiver Kontakt statt. Durch die enge Verbindung zum Dienstleister und die entstehende Abhängigkeit von der Dienstleistungsqualität ergeben sich Risiken für den Auftraggeber, durch die im schlimmsten Fall sogar die Geschäftsgrundlage des Unternehmens oder der Behörde vital gefährdet werden können (beispielsweise könnten sensitive Organisationsinformationen gewollt oder ungewollt nach außen preisgegeben werden). Der Betrachtung von Sicherheitsaspekten und der Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Outsourcing-Dienstleister kommt im Rahmen eines Outsourcing-Vorhabens somit eine zentrale Rolle zu.
Den Schwerpunkt dieses Bausteins bilden daher Maßnahmen, die sich mit IT-Sicherheitsaspekten des Outsourcings beschäftigen. Dazu zählen ebenfalls geeignete Maßnahmen zur Kontrolle der vertraglich vereinbarten Ziele und Leistungen sowie der IT-Sicherheitsmaßnahmen.

Die Gefährdungslage eines Outsourcing-Vorhabens ist ausgesprochen vielschichtig, siehe dazu 6.2.2 Gefährdungen beim Outsorcing.

15.1.1 Festlegung einer Outsourcing-Strategie

Die Bindung an einen Outsourcing-Dienstleister erfolgt auf lange Sicht, ist zunächst kostenintensiv und mit Risiken verbunden. Eine gute Planung des Outsourcing-Vorhabens ist daher wichtig. Dabei müssen neben den wirtschaftlichen, technischen und organisatorischen Randbedingungen auch die sicherheitsrelevanten Aspekte bedacht werden.

Folgende Gesichtspunkte sollten betrachtet werden:

- Unternehmensstrategie (Flexibilität, Abhängigkeiten, zukünftige Planungen),
- Machbarkeitsstudie mit Zusammenstellung der Rahmenbedingungen,
- betriebswirtschaftliche Aspekte mit Kosten-Nutzen-Abschätzung.

Nach ersten strategischen Überlegungen muss zunächst geklärt werden, welche Aufgaben oder IT-Anwendungen generell für Outsourcing in Frage kommen.

Dabei darf die Bedeutung der rechtlichen Rahmenbedingungen nicht unterschätzt werden. Gesetze könnten beispielsweise das Auslagern bestimmter Kernaufgaben einer Institution generell verbieten oder zumindest weitreichende Auflagen enthalten und die Beteiligung von Aufsichtsbehörden vorschreiben. In der Regel bleibt der Auftraggeber weiterhin gegenüber seinen Kunden oder staatlichen Stellen voll verantwortlich für Dienstleistungen oder Produkte, unabhängig davon, ob einzelne Aufgabenbereiche ausgelagert wurden.

Die IT-Sicherheit wird leider häufig zu Beginn der Planung vernachlässigt, obwohl ihr eine zentrale Bedeutung zukommt. Dies gilt sowohl für technische als auch organisatorische Sicherheitsaspekte, denen im Outsourcing-Szenario eine entscheidende Rolle zukommt. Generell ist nämlich zu bedenken:

- Die Entscheidung zum Outsourcing ist in der Regel nicht einfach zu revidieren. Die Bindung an den Dienstleister erfolgt unter Umständen sehr langfristig.
- Der Dienstleister hat Zugriff auf Daten und IT-Ressourcen des Auftraggebers. Der Outsourcing-Auftraggeber verliert dadurch die alleinige und vollständige Kontrolle über Daten und Ressourcen. Je nach Outsourcing-Vorhaben betrifft dies dann auch Daten mit hohem Schutzbedarf.
- Für die technische Umsetzung des Outsourcing-Vorhabens ist es notwendig, dass zwischen Auftraggeber und Dienstleister Daten übertragen werden. Dadurch ergibt sich automatisch ein erhöhtes Gefahrenpotenzial.
- In der Regel ist es erforderlich, dass Mitarbeiter oder Subunternehmer des Outsourcing-Dienstleisters (und damit Betriebsfremde) zeitweise in den Räumlichkeiten des Auftraggebers arbeiten müssen. Auch dadurch ergibt sich ein erhöhtes Gefahrenpotenzial.
- Im Rahmen eines Outsourcing-Vorhabens müssen neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt werden. Die Folgen der notwendigen Umstellungen müssen geklärt und abgeschätzt werden.
- Für jeden Outsourcing-Dienstleister besteht ein nicht zu unterschätzender Interessenskonflikt: Einerseits muss er die Dienstleistung möglichst kostengünstig erbringen, um seinen Gewinn zu maximieren, andererseits erwartet der Auftraggeber hohe Dienstleistungsqualität, Flexibilität und kundenfreundliches Verhalten. Dieser Punkt ist erfahrungsgemäß der am häufigsten unterschätzte. Während IT-ManagerInnen in der Regel sehr kritisch und kostenbewusst sind und Versprechungen von Herstellern und Beratern mit großer Skepsis begegnen, ist beim Outsourcing leider oft das Gegenteil zu beobachten. Allzu leicht verfällt hier der Auftraggeber den Werbeaussagen der Dienstleister in der frohen Erwartung, seine IT-Kosten signifikant senken zu können. Die Praxis lehrt jedoch, dass höchstens die Dienstleistungen in der Zukunft erbracht werden, die von Anfang an vertraglich fixiert worden sind. Stellt sich heraus, dass die Dienstleistungsqualität unzureichend ist, weil der Auftraggeber Leistungen erwartet, die er - im Gegensatz zum Outsourcing-Dienstleister - als selbstverständlich erachtet, sind Nachbesserungen in der Regel ohne hohe zusätzliche Kosten nicht zu erwarten. Alle IT-ManagerInnen, die über Outsourcing nachdenken, sollten sich die Mühe machen nachzurechnen, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit Auftraggeber und Auftragnehmer beide von dem Vertragsverhältnis profitieren. Bei dieser Rechnung stellt sich vielleicht heraus, dass eine seriöse Leistungserbringung zu den versprochenen niedrigen Kosten höchst unwahrscheinlich ist.

Um die Outsourcing-Strategie festzulegen, muss daher immer eine individuelle Sicherheitsanalyse durchgeführt werden. Nur so kann letztendlich festgestellt werden, wie bestehende IT-Systeme abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll. Schlussendlich wird dennoch ein gewisses Restrisiko durch den Outsourcing-Auftraggeber zu tragen sein. Die Ergebnisse der Sicherheitsanalyse gehen unmittelbar in die Kosten-Nutzen-Abschätzung ein.

Das Management darf bei der Entwicklung einer erfolgversprechenden, langfristigen Outsourcing-Strategie den Blick nicht nur auf die Einsparung von Kosten richten. Die Auswirkungen eines Outsourcing-Vorhabens auf die Aufgabenerfüllung, das Geschäftsmodell und das Dienstleistungs- oder Produktportfolio müssen ebenfalls berücksichtigt werden. Sollen Standardabläufe oder Kerngeschäftsprozesse ausgelagert werden? Wichtig ist in diesem Zusammenhang, dass die Fähigkeit, Anforderungen an die IT selbst zu bestimmen und zu kontrollieren in ausreichendem Maße erhalten werden. Insbesondere an die Weiterentwicklung und Pflege selbstentwickelter IT-Systeme und Anwendungen sollte gedacht werden.

Die nachfolgenden Hinweise beleuchten Vor- und Nachteile von Outsourcing mit Bezug zur IT-Sicherheit.

- Vorteil: Es besteht die Möglichkeit, neue Dienstleistungen (z. B. durch Diversifikation oder Ausweitung der Produktpalette) zu etablieren. In der Folge muss das festgelegte Sicherheitsniveau jedoch auch für das ausgeweitete Angebot sichergestellt werden.
- Vorteil: Es besteht mehr Flexibilität, beispielsweise können Systeme, Ressourcen oder der Personalbedarf schneller angepasst bzw. erweitert werden, da dies vom Outsourcing-Dienstleister unter Umständen auch kurzfristig eingekauft werden kann. Fixe Kosten können so in variable umgewandelt werden. In Folge können sich jedoch durch die Erweiterungen (z. B. von IT-Systemen) auch neue Sicherheitsprobleme ergeben.
- Vorteil: Im Idealfall kann durch das Outsourcing-Vorhaben ein besseres IT-Sicherheitsniveau erreicht werden, da der Dienstleister Spezialisten beschäftigt, so dass dadurch auch neue, sicherheitskritische Anwendungen betrieben werden können. Gerade in der IT-Sicherheit ist es sehr zeitaufwändig und benötigt viel technisches Wissen, regelmäßig die Flut an Sicherheitshinweisen, Security-Bulletins, Updatemeldungen und Bug-Reports auszuwerten, ihre Relevanz zu erkennen und bei Bedarf rasch die richtigen Schritte einzuleiten. Zunehmende Komplexität der angebotenen Hard- und Softwarelösungen, immer kürzere Produktzyklen, steigende Vernetzung und steigende Anforderungen der Nutzer machen es zudem außerordentlich schwierig, immer wieder die richtige Balance zwischen Sicherheit und „mehr Funktionalität“ zu finden.

- Vorteil: Gerade in Unternehmen oder Behörden mit kleiner IT-Abteilung haben einzelne MitarbeiterInnen oft einen hohen Stellenwert. Stehen sie einmal nicht zur Verfügung (Krankheit, Urlaub) oder verlassen die Institution, können sich gravierende Sicherheitsprobleme ergeben, weil es keinen gleichwertigen Vertreter gibt. Dienstleister hingegen können in der Regel auf mehrere gleich qualifizierte ExpertInnen zurückgreifen, die sich gegenseitig vertreten können.
- Vorteil: Von einigen Institutionen wird Outsourcing häufig als vielleicht einzige Möglichkeit gesehen, eine Neugestaltung ihrer IT-Systeme und Anwendungen gegen interne Widerstände durchzusetzen. Im Zuge des Outsourcings soll eine heterogene Systemlandschaft aufgeräumt und standardisiert werden.
- Nachteil: Wenn das Know-how der vom Outsourcing-Dienstleister eingesetzten SpezialistInnen nicht angemessen ist, so können dadurch gravierende IT-Sicherheitslücken entstehen. Ist zusätzlich intern nicht mehr das Fachwissen vorhanden, um das Sicherheitsniveau beim Outsourcing-Dienstleister zu kontrollieren, werden Sicherheitslücken womöglich nicht einmal entdeckt.
- Nachteil: Eine Ausweitung des Dienstleistungsangebots oder die Erweiterung von IT-Systemen ist nicht mehr allein eine Entscheidung des eigenen Managements. Der Outsourcing-Dienstleister muss immer an der Diskussion beteiligt werden. Dienstleister kompensieren nicht selten günstige Konditionen bei Vertragsabschluss durch hohe Forderungen bei späteren Sonderwünschen oder neuen Anforderungen des Auftraggebers. Der dann entstehende Kostendruck führt oftmals zu Einsparungen bei der IT-Sicherheit.
- Nachteil: Der Aufwand für die Kontrolle der Dienstleistungsqualität darf nicht unterschätzt werden. Sollten hierbei Defizite festgestellt werden, können diese schwierig und zeitaufwendig zu beheben sein, vor allem wenn es zu Meinungsverschiedenheiten zwischen Auftraggeber und Dienstleister kommt. Wenn Fragen der IT-Sicherheit dann nicht zeitnah gelöst werden, können sich Sicherheitslücken ergeben.

Eine umfassende Kosten-Nutzen-Analyse jedes Outsourcing-Vorhabens ist essentiell für den strategischen und wirtschaftlichen Erfolg. Es ist daher wichtig, alle Parameter zu kennen und auch richtig einzuschätzen.

Der strategische Wert der folgenden Ressourcen muss unter den Rahmenbedingungen des Outsourcing-Vorhabens eingeschätzt werden:

- Know-how
- MitarbeiterInnen
- IT-Systeme und Anwendungen

Bei der Kosten-Nutzen-Analyse können Studien und Erfahrungsberichte anderer Institutionen wertvolle Informationen liefern.

Abschließend ist die Outsourcing-Strategie zu dokumentieren. Die Ziele, Chancen und Risiken des Outsourcing-Vorhabens sollten eindeutig beschrieben werden.
Es empfiehlt sich unter diesem Gesichtspunkt außerdem, die im Rahmen eines laufenden Outsourcing-Vorhabens gemachten Erfahrungen in die Dokumentation der Outsourcing-Strategie zu integrieren. Es sollte dabei auch auf Fehlentscheidungen und daraus abgeleitete Empfehlungen für die Zukunft hingewiesen werden.

15.1.2 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

Wenn eine Outsourcing-Strategie festgelegt wurde, müssen die IT-Sicherheitsanforderungen so konkret ausgearbeitet werden, dass auf ihrer Basis der geeignete Dienstleister ausgesucht werden kann. Dabei sind Sicherheitsanforderungen an den Outsourcing-Dienstleister selbst, die benutzte Technik (inklusive Kommunikationswege und -dienste), aber auch an die eigene Organisation zu stellen.

Die Erstellung eines detaillierten Sicherheitskonzeptes, das auf den hier formulierten Anforderungen aufbaut und nach Auswahl des Dienstleisters ausgearbeitet wird, wird in 15.1.5 Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben beschrieben.

Es ist zu bedenken, dass das Festlegen von IT-Sicherheitsanforderungen ein iterativer Prozess ist:

- Zunächst werden die gewünschten IT-Sicherheitsanforderungen durch den Auftraggeber spezifiziert.
- Danach wird in der Angebotsphase abgeglichen, wie und ob die gewünschten IT-Sicherheitsanforderungen durch die anbietenden Dienstleister geleistet werden können (siehe auch 15.1.3 Wahl eines geeigneten Outsourcing-Dienstleisters).
- Ist ein Dienstleister ausgewählt, so muss mit diesem die weitere Verfeinerung der IT-Sicherheitsanforderungen (z. B. basierend auf den eingesetzten Betriebssystemen oder Sicherheitsmechanismen) erarbeitet werden.
- In der Endphase dieses Abstimmungsprozesses müssen dann auch die Sicherheitsanforderungen für die konkrete Umsetzung definiert werden.

Generell ergeben sich für Outsourcing-Szenarien folgende Mindestsicherheitsanforderungen:

- Die Umsetzung der Anforderungen des Sicherheitshandbuchs ist eine Minimalforderung an beide Outsourcing-Parteien. Zusätzlich müssen sowohl Outsourcing-Dienstleister als auch der Auftraggeber selbst ein IT-Sicherheitskonzept besitzen und dieses umgesetzt haben.
- Es ist wichtig, die relevanten IT-Verbünde genau abzugrenzen (z. B. nach Fachaufgabe, Geschäftsprozess, IT-Systemen), so dass alle Schnittstellen identifiziert werden können. An die Schnittstellen können dann entsprechende technische Sicherheitsanforderungen gestellt werden.
- Es muss eine Ist-Strukturanalyse von IT-Systemen und Anwendungen (siehe auch 15.1.1 Festlegung einer Outsourcing-Strategie) erfolgen.
- Es muss eine Schutzbedarfsfeststellung (z. B. von Anwendungen, Systemen, Kommunikationsverbindungen, Räumen) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit erfolgen (siehe auch 15.1.1 Festlegung einer Outsourcing-Strategie).

Natürlich sind auch relevante Gesetze und Vorschriften zu beachten. Dies kann besonders in Fällen, in denen Auftraggeber oder Dienstleister länderübergreifend oder weltweit operieren, aufwendig sein.

Im Rahmen der IT-Sicherheitsanforderungen ist festzulegen, welche Rechte (z. B. Zutrittsrechte, Zugriffsrechte auf Daten und Systeme) dem Outsourcing-Dienstleister vom Auftraggeber eingeräumt werden.

Die Anforderungen an Infrastruktur, Organisation, Personal und Technik müssen beschrieben werden. Es genügt hier oftmals die Verpflichtung auf ein Sicherheitsniveau, das diesem Sicherheitshandbuch entspricht. Sollten darüber hinausgehende Anforderungen bestehen, müssen diese detailliert beschrieben werden. Dies hängt entscheidend von der Sicherheitsstrategie und bereits vorhandenen Systemen und Anwendungen ab. Beispielsweise könnten folgende Punkte in Abhängigkeit vom Outsourcing-Vorhaben detailliert werden:

- Anforderungen an sicherheitskritische organisatorische Prozesse (z. B. Zeitrestriktionen für den Alarmierungsplan) können spezifiziert werden.
- Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein CISO mit speziellen Kenntnissen (z. B. Host-Kenntnissen) beim Outsourcing-Dienstleister benannt werden muss
- Der Einsatz zertifizierter Produkte (z. B. gemäß [Common Criteria]) beim Outsourcing-Dienstleister kann gefordert werden.
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen können gestellt werden. Beispielsweise kann in diesem Zusammenhang der Grad und die Methode der Lastverteilung (z. B. für Web-Server mit Kundenzugriff bei sehr vielen Kunden) vorgegeben werden.

- Vorgaben an die Mandantenfähigkeit sowie die diesbezügliche Trennung von Hard- und Software können formuliert werden. Beispielsweise kann festgelegt werden, dass keine IT-Systeme des Auftraggebers in Räumen untergebracht werden dürfen, in denen bereits Systeme anderer Mandanten des Dienstleisters stehen.
- Spezielle Verfahren zur Absicherung der Kommunikation zwischen Dienstleister und Auftraggeber wie Einsatz von Verschlüsselungs- und Signaturverfahren können fest vorgegeben werden.
- Allgemeine Anforderungen bezüglich Kontrolle und Messung von Sicherheit, Qualität oder auch Abläufen und organisatorischen Regelungen können festgelegt werden, z. B. Zeitintervalle, Zuständigkeiten.
- Gewünschte Verfahren oder Mechanismen für die Kontrolle und Überwachung, wie unangekündigte Kontrollen vor Ort, Audits (unter Umständen durch unabhängige Dritte) können spezifiziert werden.
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien können festgelegt werden.

Generell bilden die festgelegten IT-Sicherheitsanforderungen eine der Grundlagen für die Wahl eines geeigneten Outsourcing-Dienstleisters. Spezielle IT-Sicherheitsanforderungen müssen jedoch eventuell an das von Dienstleistern umsetzbare IT-Sicherheitsniveau angepasst werden.

15.1.3 Wahl eines geeigneten Outsourcing-Dienstleisters

Bei der Wahl eines geeigneten Outsourcing-Dienstleisters sind ein möglichst detailliertes Anforderungsprofil und ein darauf basierendes Pflichtenheft entscheidende Erfolgsfaktoren. Nur so kann eine bedarfsgerechte Ausschreibung erfolgen, auf die sich auch geeignete Dienstleister bewerben.

die Ausschreibung sollte

- die Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung) sowie
- die Beschreibungen zum geforderten Qualitätsniveau, welches nicht zwangsläufig dem Niveau des Auftraggebers entsprechen muss,

enthalten.

Weiters müssen den potenziellen Dienstleistern auch möglichst detailliert

- die IT-Sicherheitsanforderungen und
- die Kriterien zur Messung von Servicequalität und Sicherheit

mitgeteilt werden (siehe 15.1.2 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben). In Einzelfällen kann es notwendig sein, die Detailanforderungen bezüglich Sicherheit nur gegen eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement) an Dienstleister herauszugeben, da sich daraus Hinweise auf existierende oder geplante Sicherheitsmechanismen ableiten lassen.

Das Anforderungsprofil hängt stark von der Art des Outsourcing-Vorhabens ab. Als wichtige grundsätzliche Bewertungskriterien für Dienstleister und dessen Personal können gelten:

- Bei ausländischen Dienstleistern müssen besondere Aspekte bedacht werden. Dazu gehören beispielsweise: fremde Gesetzgebung, andere Haftungsregelungen, Spionagerisiko, andere Sicherheitskultur, im Partnerunternehmen bzw. durch die landesspezifische Gesetzgebung zugelassene und verwendbare Sicherheitsmechanismen.
- Die Größe des Dienstleisters kann bei der Auswahl ein Argument sein. Bei kleinen Unternehmen könnte das Insolvenzrisiko höher sein. Bei großen Unternehmen ist zu bedenken, dass diese sehr viele Auftraggeber und Projekte haben, so dass ein einzelner Auftraggeber nur einer unter vielen ist und keine bevorzugte Stellung einnimmt.
- Der Dienstleister sollte Referenzen für ähnliche Outsourcing-Vorhaben aufweisen können. Dabei ist auf Interessenskonflikte durch Geschäftsbeziehungen zu Konkurrenten des Auftraggebers und auf die Unabhängigkeit von bestimmten Herstellern (z. B. Zulieferer, die Konkurrenten des Auftraggebers sind) zu achten.
- Die Organisationsform eines Dienstleisters kann in Betracht gezogen werden, da dies z. B. die Haftungsgrenzen beeinflussen kann. Die Eigentümerstruktur sollte recherchiert werden, um mögliche Einflussfaktoren im Vorfeld abzuklären.
- Die Kundenstruktur sollte beachtet werden, da dies darauf hinweist, in welchem Wirtschaftssektor der Anbieter seine Stärken hat.
- Ein Qualitätsnachweis bzw. eine Zertifizierung, z. B. nach ISO/IEC 27001 oder ISO 9000, ist eine sinnvolle Forderung.
- Auskünfte über die aktuelle wirtschaftliche Lage sowie Erwartungen an die zukünftige Geschäftsentwicklung der Dienstleister sollten eingeholt werden.

Auch an die MitarbeiterInnen eines Dienstleisters sind diverse Anforderungen zu stellen (siehe auch 7.2 Regelungen für den Einsatz von Fremdpersonal).

- Die Qualifikation der MitarbeiterInnen muss in die Bewertung der Angebote einfließen. Es ist nach der Projektvergabe darauf zu achten, dass die im Angebot genannten MitarbeiterInnen auch später tatsächlich eingesetzt werden.
- Die Anzahl der verfügbaren MitarbeiterInnen muss bewertet werden. Dabei sollten auch die Vertretungsregelungen und die Arbeitszeiten hinterfragt werden.

- Bei der Wahl ausländischer Partner muss eine gemeinsame Sprache für die Kommunikation zwischen den eigenen MitarbeiterInnen und denen des Dienstleisters festgelegt werden. Hierbei sollte auch hinterfragt werden, ob die vorhandenen Sprachkenntnisse für die Klärung von Detailproblemen ausreichen. Die Erfahrungen zeigen, dass viele Personen aus Angst, sich zu blamieren, lieber zu wichtigen Fragen schweigen, wenn sie ihre Sprachfähigkeiten als nicht perfekt einschätzen.
- Entsprechend dem erforderlichen Sicherheitsniveau für das Outsourcing-Vorhaben sollte in die Bewertung der Angebote mit aufgenommen werden, ob eine Sicherheitsüberprüfung der MitarbeiterInnen vorliegt bzw. eine solche durchgeführt werden kann.

15.1.4 Vertragsgestaltung mit dem Outsourcing-Dienstleister

Nachdem ein Outsourcing-Dienstleister ausgewählt wurde, müssen alle Aspekte des Outsourcing-Vorhabens vertraglich in sogenannten Service Level Agreements (SLAs) festgehalten und geregelt werden. Die Aspekte, die im Folgenden beschrieben werden, sind als Hilfsmittel und Checkliste bei der Vertragsgestaltung zu sehen. Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen immer vom speziellen Outsourcing-Projekt ab. Je höher der Schutzbedarf der ausgelagerten IT-Systeme und Anwendungen ist, desto sorgfältiger und detaillierter muss der Vertrag zwischen Auftraggeber und Dienstleister ausgehandelt werden.

Der Dienstleister sollte zur Einhaltung des Sicherheitshandbuchs und auf die vom Auftraggeber vorgegebenen Sicherheitsanforderungen verpflichtet werden (siehe 15.1.2 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben). Dazu gehört natürlich, dass der Outsourcing-Dienstleister sich verpflichtet, ein IT-Sicherheitskonzept inklusive eines Notfallvorsorgekonzepts zu erstellen und Sicherheitsmaßnahmen sowie Systeme und Anwendungen zu dokumentieren.

Zusätzlich zur allgemeinen Leistungsbeschreibung empfiehlt es sich jedoch immer, auch eine genaue quantitative Leistungsbeschreibung vertraglich zu fixieren, z. B. zu Verfügbarkeitsanforderungen, Reaktionszeiten, Rechenleistung, zur Verfügung stehendem Speicherplatz, Anzahl der MitarbeiterInnen, Supportzeiten.

Generell wäre eine allgemeine Verpflichtung auf die Einhaltung des Sicherheitshandbuchs zwar zufriedenstellend, es empfiehlt sich jedoch immer, alle vereinbarten Leistungen so genau und eindeutig wie möglich vertraglich festzuhalten. Dadurch lassen sich später Streitigkeiten zwischen den Parteien vermeiden. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretationen der beschriebenen Leistungen notwendig werden,

sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden. Auch die Erstellung des IT-Sicherheitskonzeptes selbst sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen.

Im Folgenden findet sich eine Themenliste von Aspekten, die aus Sicherheitssicht geregelt werden sollten:

Infrastruktur

- Absicherung der Infrastruktur des Dienstleisters (z. B. Zutrittskontrolle, Brandschutz, …)

Organisatorische Regelungen/Prozesse

- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
    - Verfahren zur Behebung von Problemen, Benennung von AnsprechpartnerInnen mit den nötigen Befugnissen
    - regelmäßige Abstimmungsrunden
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Zugriffsmöglichkeiten des Dienstleisters auf IT-Ressourcen des Auftraggebers: Wer greift wie auf welches System zu? Wie sind die Zuständigkeiten und Rechte?
- Zutritts- und Zugriffsberechtigungen für MitarbeiterInnen des Dienstleisters zu den Räumlichkeiten und IT-Systemen des Auftraggebers
- Zutritts- und Zugriffsberechtigungen für MitarbeiterInnen des Auftraggebers zu den Räumlichkeiten und IT-Systemen des Dienstleisters

Personal

- Gestaltung der Arbeitsplätze von externen MitarbeiterInnen (Einhalten von Computerarbeitsplatzrichtlinien)
- Festlegung und Abstimmung von Vertretungsregelungen
- Verpflichtung zu Fortbildungsmaßnahmen

Notfallvorsorge

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- erforderliche Handlungen beim Eintreten eines Störfalls
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Auftraggebers bei der Behebung von Notfällen

- Art und zeitliche Abfolge von regelmäßigen und adäquaten Notfallübungen
- Art und Umfang der Datensicherung
- Vereinbarung, ob bzw. welche Systeme redundant ausgelegt sein müssen
- Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Es sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Dienstleisters die Verfügbarkeit von Daten und Systemen sichergestellt werden kann. Besonders wenn Dienstleister und Auftraggeber unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Auftraggeber von derartigen Vorkommnissen gänzlich überrascht werden.

Haftung, juristische Rahmenbedingungen

- Eine Verpflichtung auf die Einhaltung von geltenden Normen und Gesetzen sowie der vereinbarten Sicherheitsmaßnahmen und sonstigen Rahmenbedingungen ist vertraglich zu regeln. Ebenso sind Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) vertraglich zu fixieren.
- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvolle Regelungen festzulegen.
- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist auch zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- Regelungen für das Ende des Outsourcing-Vorhabens, z. B. für einen Wechsel oder bei Insolvenz des Dienstleisters, können spezifiziert werden. Auf ein ausreichend flexibles Kündigungsrecht ist zu achten.
- Der Auftragnehmer ist zu verpflichten, nach Beendigung des Auftrags alle Hard- und Software inklusive gespeicherter Daten, die dem Auftraggeber gehören, zurückzugeben. Alle vorhandenen Daten inklusive Datensicherungen sind ebenfalls zurückzugeben oder (je nach Vereinbarung) zu vernichten.
- Die Aufteilung von Risiken zwischen Auftraggeber und Dienstleister muss bedacht werden.
- Haftungsfragen im Schadensfall sind zu klären.
- Sanktionen oder Schadensersatz bei Nichteinhaltung der Dienstleistungsqualität müssen festgelegt werden. Die Bedeutung von Schadensersatzzahlungen und juristischen Konsequenzen sollte dabei nicht überschätzt werden. Zu bedenken sind nämlich die folgenden Punkte

    1. Quantifizierbarkeit des Schadens

        - Wie wird beispielsweise ein Imageschaden gemessen?

    - Wie ist es zu bewerten, wenn gravierende Pflichtverletzungen aufgedeckt werden, die nur zufällig nicht zu einem größeren Schaden geführt haben?
2. Insolvenz des Dienstleisters
   Das Recht auf Schadensersatzzahlungen ist wertlos, wenn diese die Zahlungsfähigkeit des Dienstleisters übersteigen und dieser Insolvenz anmeldet. Nachfolgend fallen dann mindestens Kosten für den Umzug zu einem neuen Dienstleister an.
3. Katastrophale Schäden
   Eine Konventionalstrafe kommt zu spät, wenn der Auftraggeber durch das Ausmaß des Schadensereignisses seiner Geschäftsgrundlage beraubt wird und im schlimmsten Fall durch die Schadensfolgen die Zahlungsunfähigkeit eintritt.
4. Kann ein Schaden nachgewiesen bzw. der Verursacher überführt werden (z. B. Nachweis von Spionage oder Manipulationen)?

Es ist immer zu bedenken, dass Schadensersatzzahlungen nur das allerletzte Mittel sind und nicht dazu führen dürfen, dass aus Kostengründen andere Sicherheitsmaßnahmen vernachlässigt werden. Sicherheit lässt sich nicht mit juristischen Mitteln erzielen.

Mandantenfähigkeit

- Die notwendige Trennung von IT-Systemen und Anwendungen verschiedener Kunden muss vereinbart werden.
    - Es ist sicherzustellen, dass Probleme bei anderen Kunden nicht die Abläufe und Systeme des Auftraggebers beeinrächtigen.
    - Es ist sicherzustellen, dass Daten des Auftraggebers unter keinen Umständen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden.
- Falls notwendig, muss die physikalische Trennung (d. h. dezidierte Hardware) vereinbart werden.
- Falls notwendig, muss vereinbart werden, dass die vom Dienstleister eingesetzten Mitarbeiter nicht für andere Auftraggeber eingesetzt werden. Es kann auch sinnvoll sein, diese auf Verschwiegenheit zu verpflichten, so dass die eingesetzten MitarbeiterInnen nicht mit anderen MitarbeiterInnen des Dienstleisters auftraggeberbezogene Informationen austauschen dürfen.

Änderungsmanagement und Testverfahren

- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Auftraggeber immer in der Lage ist, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn beispielsweise gesetzliche Vorgaben geändert wurden. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert wird.

- In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener Systeme zu regeln. Nicht selten übernimmt der Dienstleister selbstentwickelte Systeme oder Software vom Auftraggeber, der damit die Fähigkeit verliert, diese in seinem Sinne weiterzuentwickeln. Der Evolutionspfad von Systemen muss daher geregelt werden.
- Eine kontinuierliche Verbesserung der Dienstleistungsqualität und des IT-Sicherheitsniveaus sollte bereits in den SLAs (Service Level Agreements) festgeschrieben werden.
- Der Zeitrahmen für die Behebung von Fehlern ist festzulegen.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
    - Regelungen für Updates und Systemanpassungen
    - Trennung von Test- und Produktionssystemen
    - Zuständigkeiten bei der Erstellung von Testkonzepten
    - Festlegen von zu benutzenden Testmodellen
    - Zuständigkeiten bei Auftraggeber und Dienstleister bei der Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Auftraggebers, Abnahme- und Freigabeprozeduren)
    - Informationspflicht und Absprache vor wichtigen Eingriffen ins System (Negativbeispiel: Der Dienstleister spielt ein neues Betriebssystem auf dem Server ein. Durch unerwartete Fehler dabei werden wichtige Anwendungen gestört, ohne dass der Auftraggeber sich vorbereiten konnte.)
    - Genehmigungsverfahren für die Durchführung von Tests
    - Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit)

Kontrollen

- Dienstleistungsqualität und IT-Sicherheit müssen regelmäßig kontrolliert werden. Der Auftraggeber muss die dazu notwendigen Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte besitzen. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies bereits im Vertrag geregelt sein.
- Allen Institutionen, die beim Auftraggeber Prüfungen durchführen müssen (z. B. Aufsichtsbehörden) müssen auch beim Outsourcing-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) eingeräumt werden.

15.1.5 Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

Für jedes Outsourcing-Vorhaben muss ein IT-Sicherheitskonzept existieren. Dieses kann unter anderem auf Grundlage dieses Sicherheitshandbuchs erstellt sein. Outsourcing-Projekte sind dadurch gekennzeichnet, dass sich viele technische und organisatorische Details erst im Laufe der Planung und bei Migration der Systeme ergeben. Das IT-Sicherheitskonzept, das nach Beauftragung eines Dienstleisters erarbeitet wird, wird daher in den wenigsten Fällen gleich vollständig und endgültig sein und muss während der Migrationsphase von allen Beteiligten stetig weiterentwickelt und konkretisiert werden.

Generell unterscheiden sich IT-Sicherheitskonzepte für Outsourcing-Vorhaben nur wenig von IT-Sicherheitskonzepten für selbstbetriebene IT-Systeme. Es ergeben sich jedoch folgende Besonderheiten, die berücksichtigt werden müssen:

- Am Outsourcing-Vorhaben sind aus technischer Sicht in der Regel drei Parteien beteiligt:
    1. der Outsourcing-Auftraggeber,
    2. der Dienstleister und
    3. der Netzprovider (dieser stellt die Anbindung zwischen den Outsourcing-Parteien bereit. Die Zuständigkeit für die Netzanbindung fällt dabei in der Regel dem Outsourcing-Dienstleister zu).
- Jeder Beteiligte muss ein eigenes IT-Sicherheitskonzept erstellen und umsetzen, welches auch das spezielle Outsourcing-Vorhaben umfasst. Damit sind IT-Sicherheitskonzepte erforderlich:
    - für den Einflussbereich des Outsourcing-Dienstleisters,
    - für den Einflussbereich des Auftraggebers sowie
    - für die Schnittstellen und die Kommunikation zwischen diesen Bereichen.
- Zusätzlich zu den Einzelkonzepten ist ein IT-Sicherheitskonzept für das Gesamtsystem zu erstellen, welches die Sicherheit im Zusammenspiel der Einzelsysteme betrachtet.
- Die verschiedenen Teil-Konzepte müssen zwischen Auftraggeber und Dienstleistern abgestimmt werden. Dabei ist der Auftraggeber am IT-Sicherheitskonzept des Outsourcing-Dienstleisters nicht direkt beteiligt, sollte aber in einem Audit prüfen, ob es vorhanden und ausreichend ist. Für das Audit kann der Auftraggeber dabei auch auf externe Dritte zurückgreifen.

Die in 15.1.2 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben und 15.1.4 Vertragsgestaltung mit dem Outsourcing-Dienstleister genannten Sicherheitsanforderungen bilden dabei die Basis für das IT-Sicherheitskonzept. Aufbauend auf den dort beschriebenen grundlegenden Anforderungen muss im IT-Sicherheitskonzept die detaillierte Ausgestaltung erfolgen, wobei beispielsweise die Maßnahmen konkretisiert und Ansprechpartner namentlich festgelegt werden.

Erfahrungsgemäß ist der Übergang (Migration) von Aufgaben und IT-Systemen vom Auftraggeber zum Outsourcing-Dienstleister eine Projektphase, in der verstärkt mit Sicherheitsvorfällen zu rechnen ist. Aus diesem Grund müssen im Sicherheitskonzept Regelungen und Maßnahmen zur Migration behandelt werden:

- Es ist ein gemischtes Team aus MitarbeiterInnen des Auftraggebers und des Outsourcing-Dienstleisters zu bilden. Dieses kann auch durch externe ExpertInnen verstärkt werden, um spezielles Know-how verfügbar zu machen.
- Für die Migrationsphase muss eine IT-Sicherheitskonzeption erstellt werden.
- Die Verantwortlichkeiten und Hierarchien für die Migrationsphase sind festzulegen. Dabei ist es wichtig, dass klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige AnsprechpartnerInnen definiert werden. Zusätzlich ist darauf zu achten, dass auf beiden Seiten Verantwortlichkeiten auch auf hohen Ebenen definiert werden. Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.
- Die erforderlichen Tests müssen geplant und durchgeführt werden, Abnahmeprozeduren erarbeitet und die Produktionseinführung geplant werden.
- Es sind geeignete interne MitarbeiterInnen für die Test-, Einführungsphase und den späteren Betrieb auszuwählen. Vertraglich kann sich ein Auftraggeber natürlich auch ein Mitspracherecht bei der Personalauswahl des Outsourcing-Dienstleisters einräumen lassen.
- Die MitarbeiterInnen des Auftraggebers sind zum Verhalten während und nach der Migrationsphase zu schulen. In der Regel sind die MitarbeiterInnen dabei mit neuen und unbekannten AnsprechpartnerInnen konfrontiert. Dies birgt die Gefahr des „Social Engineerings“ (z. B. Anruf eines vermeintlichen Mitglieds des Sicherheitsteams des Dienstleisters).
- Der Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Auftraggebers genau kennen lernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen. Die produktiven Systeme dürfen dabei nicht vernachlässigt werden. Dazu ist im Vorfeld zu überprüfen, ob die vorgesehenen MitarbeiteInnenr zur Verfügung stehen. Zusätzlich müssen Störungen durch notwendige Tests einkalkuliert werden.

- Anwendungen und IT-Systeme, die der Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit muss dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch das Outsourcing-Vorhaben. Die Dokumentation neuer Systeme oder Teilsysteme muss dabei ebenfalls sichergestellt sein.
- Während der Migration muss ständig überprüft werden, ob die SLAs oder die vorgesehenen IT-Sicherheitsmaßnahmen angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen eingestellt hat, sind verstärkt MitarbeiterInnen zu Bereitschaftsdiensten zu verpflichten.

Nach Abschluss der Migration muss sichergestellt werden, dass das IT-Sicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- AnsprechpartnerInnen und Zuständigkeiten werden mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert.
- Die Systemkonfigurationen ist zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.

Als letzte Aufgabe muss das Outsourcing-Vorhaben nach der Migrationsphase in den sicheren Regelbetrieb überführt werden. Dabei ist vor allem darauf zu achten, dass alle Ausnahmeregelungen, die während der Migrationsphase notwendig waren, wie z. B. erweiterte Zugriffsrechte, aufgehoben werden.

Im Folgenden sind einige Aspekte und Themen aufgelistet, die im IT-Sicherheitskonzept im Detail beschrieben werden sollten. Da die Details eines IT-Sicherheitskonzeptes direkt vom Outsourcing-Vorhaben abhängen, ist die Liste als Anregung zu verstehen und erhebt keinen Anspruch auf Vollständigkeit. Neben einem Überblick über die Gefährdungslage, die der Motivation der Sicherheitsmaßnahmen dient, und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

Organisation

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen/Vernichten
- Festlegung von Aktionen, für die das „Vier-Augen-Prinzip“ anzuwenden ist

Hard-/Software

- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
- Einsatz von Datei-Integrität-Prüfungssystemen, um Veränderungen z. B. nach erfolgreichen Angriffen, zu erkennen
- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
- Einsatz kaskadierter Firewallsysteme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters
- sorgfältige Vergabe von Benutzerkennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters

Kommunikation

- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Auftraggeber, um sensitive Daten zu schützen
- Authentisierungsmechanismen
- Detailregelungen für weitere Netzanbindungen (siehe 14.7.1 Richtlinien bei Verbindung mit Netzen Dritter (Extranet))
- Detailregelungen für den Datenaustausch (siehe 13.2.1 Richtlinien beim Datenaustausch mit Dritten)

Kontrollen und QS

- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Sicherheit, Dienstqualität, Abläufen und organisatorische Regelungen

Notfallvorsorge

- Das Notfallvorsorgekonzept ist in 15.1.6 Notfallvorsorge beim Outsourcing beschrieben.

15.1.6 Notfallvorsorge beim Outsourcing

Für die Notfallvorsorge beim Outsourcing gelten grundsätzlich die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb von IT-Systemen. Die Besonderheiten beim Outsourcing-Betrieb ergeben sich dadurch, dass auch die Notfallvorsorge auf unterschiedliche Parteien aufgeteilt ist und durch die Verteilung der IT-Komponenten auch zusätzliche Komponenten neu hinzukommen.

Generell müssen Notfallvorsorgekonzepte für die Systeme beim Auftraggeber, beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Auftraggeber und Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren. In 15.1.4 Vertragsgestaltung mit dem Outsourcing-Dienstleister sind einige Hinweise gegeben, welche Aspekte bereits im Service Level Agreement geregelt werden sollten. Im Notfallvorsorgekonzept müssen diese Vorgaben genau spezifiziert und im Detail beschrieben werden:

- Zuständigkeiten, AnsprechpartnerInnen und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
- Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.

Die IT-Sicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Outsourcing-Dienstleisters ab. Oftmals werden die Systeme des Auftraggebers von Personal des Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die Anwendung liegt dennoch ausschließlich beim Auftraggeber. Tritt ein Fehler in der Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das System zu besitzen. Durch das Notfallvorsorgekonzept müssen dem Outsourcing-Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden, wie er dabei vorgehen darf. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot einer Maschine).

Ein Fehlverhalten einer Anwendung kann technische Ursachen haben (z. B. Datenträger voll, Netzprobleme) oder anwendungsspezifische (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung).

Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können. Meist ist aber dennoch eine Kooperation mit dem Auftraggeber notwendig, um ungewünschte Seiteneffekte auf Applikationsebene zu verhindern.

Liegen anwendungsspezifische Probleme vor, benötigt der Outsourcing-Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit Ansprechpartnern auf Seiten des Auftraggebers, damit er richtig reagieren kann. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Auftraggeber vorhanden sind.

Wichtig ist in diesem Fall auch, dem Dienstleister Informationen bezüglich des Schutzbedarfs der betroffenen Daten und Systeme zur Verfügung zu stellen, damit mit angemessener Umsicht gehandelt werden kann.

15.2 Angriffe auf die Lieferkette

Als sogenannte „Supply Chain-Angriffe“ (auch: Angriffe auf die Lieferkette) werden Attacken bezeichnet, bei denen ein Zulieferbetrieb oder externe Dienstleister in der Lieferkette angegriffen werden und dieser Zulieferbetrieb ist nicht das endgültige Angriffsziel. Das bedeutet auch Zulieferbetriebe von Zulieferbetrieben können Angriffsziele darstellen. Solche Angriffe werden dazu missbraucht Zugang auf andere Systeme oder in Organisationen zu erhalten, diese sind dann sogenannte „Final-Targets“.

Erfahrungsgemäß ist die praktische Ausgangslage für einen solchen Angriff in den meisten Fällen das Prinzip, das schwächste Glied in der Sicherheitskette zuerst zu identifizieren und anschließend nach geeigneter Vorbereitung auch anzugreifen, um zu einem späteren Zeitpunkt das zumeist besser geschützte „Final-Target“ anzugreifen. Die Grundlage dafür ist, dass viele auf Unterstützung meist kleinerer und in Bezug auf Cyber Security manchmal auch weniger gut geschützte Outsourcing-Partner für die Erbringung von Dienstleistungen bzw. für die Produktion setzen. Ursache dafür kann beispielsweise die Spezialisierung auf Teilbereiche sein.

Supply-Chain-Angriffe sind üblicherweise nicht ausschließlich auf die Verwendung manipulierter Firmware bzw. Software beschränkt. Das bedeutet, dass die manipulierten software-intensiven Systeme sowohl aus reiner Software bestehen können, aus Hardware sowie aber auch aus einer integrierten Kombination daraus (Software und Hardware). Auch ist die Ebene auf der die Software ein Angriffsziel sein kann nicht eingeschränkt. Demzufolge kann sowohl Firmware ein Angriffsziel darstellen aber auch konventionelle Webapplikationen. Gemeinsam haben diese Arten von Supply-Chain-Angriffen, dass sehr oft legitime Firmware oder anderer Source-Code etwa für Webapplikationen als Träger für die Verbreitung von Schadsoftware missbraucht werden.

Vor diesem Hintergrund greift ein Gegner einen Outsourcing-Partner böswillig oder versehentlich an. Ziel des Angriffs ist es, manipulierte software-intensive Systeme bzw. Bausteine für eine üblicherweise spätere Ausnutzung im Lebenszyklus des Produkts in der IT-Infrastruktur des Outsourcing-Partners unterzubringen. Darüber hinaus erfolgt zu einem späteren Zeitpunkt im Lebenszyklus die Aktivierung der in das System oder in einen Baustein eingebrachten Schadsoftware.

Laut BSI (OPS.2.1: Outsourcing für Kunden) ergibt sich die folgende Bedrohungslage, welche sich auf die Sicherheitsziele der Organisation auswirkt. Auch bei der Auslagerung von Geschäftsprozessen oder Dienstleistungen an einen Outsourcing-Dienstleister soll die Erfüllung der Sicherheitsziele möglich sein:

- Fehlende oder unzureichende Regelungen zur Informationssicherheit
- Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten
- Fehlendes oder unzureichendes Test- und Freigabeverfahren
- Unzulängliche vertragliche Regelungen mit Outsourcing-Dienstleistern
- Unzulängliche Regelungen für das Ende eines Outsourcings
- Abhängigkeit von einem Outsourcing-Dienstleister
- Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
- Mangelhafte Informationssicherheit in der Einführungsphase von Outsourcing
- Ausfall der Systeme eines Outsourcing-Dienstleisters
- Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
- Fehlende Mandantenfähigkeit beim Outsourcing-Dienstleister

Darüber hinaus definiert der BSI OPS.2.1 die folgenden elementaren Gefährdungen:

- Ausfall oder Störung von Dienstleistern
- Ausspähen von Informationen (Spionage)
- Abhören
- Verlust von Geräten, Datenträgern oder Dokumenten
- Fehlplanung oder fehlende Anpassung
- Offenlegung schützenswerter Informationen
- Manipulation von Informationen
- Ausfall von Geräten oder Systemen
- Verstoß gegen Gesetze oder Regelungen
- Nötigung, Erpressung oder Korruption
- Social Engineering

Aus diesen Gefährungen ergeben sich die nachfolgend dargestellten Sicherheitsanforderungen in drei Kategorien: Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf.

Die nach dem BSI zwingend zu erfüllende Basisanforderung ist:

- Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben (Basis)

Darüber hinaus sind Standard-Anforderungen durch das BSI festgelegt, die gemeinsam mit der zuvor genannten Basisanforderung dem Stand der Technik entsprechen.

- Rechtzeitige Beteiligung der Personalvertretung
- Auswahl eines geeigneten Outsourcing-Dienstleisters
- Vertragsgestaltung mit dem Outsourcing-Dienstleister
- Festlegung einer Strategie zum Outsourcing
- Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben
- Festlegung der möglichen Kommunikationspartner
- Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters
- Vereinbarung über die Anbindung an Netze der Outsourcing-Partner
- Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern
- Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
- Änderungsmanagement
- Sichere Migration bei Outsourcing-Vorhaben
- Notfallvorsorge beim Outsourcing
- Geordnete Beendigung eines Outsourcing-Verhältnisses

Neben den zuvor beschriebenen Standard-Anforderungen ergibt sich für einen erhöhten Schutzbedarf zusätzlich noch die folgende Anforderung:

- Sicherheitsüberprüfung von Mitarbeitern (idealerweise vor der Anstellung oder vor der Beauftragung abgewickelt)

[Quelle: BSI OPS.2.1: Outsourcing für Kunden]

16 Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)

Sicherheitsrelevante Ereignisse bzw. Informationssicherheitsereignisse gemäß ISO/IEC 27002 sind generell alle unerwünschten Vorkommnisse, die Sicherheitsprobleme aufdecken resp. dann Sicherheitsvorfälle nach sich ziehen oder dies können. Dazu zählen etwa Einbruchsversuche in das System (Hacking), das Auftreten von Schadprogrammen aber auch das Erkennen von Schwachstellen mit entsprechendem Gefahrenpotenzial.

Als Sicherheitsvorfall wird ein Informationssicherheitsereignis bezeichnet, das konkrete Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden verursacht oder nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten sein.

Auch wenn in diesem Handbuch der Schwerpunkt auf der Informationstechnologie liegt, sind bei der Behandlung von IT-Sicherheitsvorfällen Überschneidungen zu Vorfällen in anderen Bereichen ebenso zu beachten.

16.1 Reaktion auf Sicherheitsvorfälle bzw. sicherheitsrelevante Ereignisse (Incident Handling)

Auch bei Vorhandensein wirksamer Sicherheitsmaßnahmen und eines hohen Sicherheitsniveaus ist das Auftreten solcher Ereignisse nicht gänzlich zu verhindern. Jede Institution muss ein vitales Interesse daran haben, dass auf sicherheitsrelevante Ereignisse so schnell und effektiv wie möglich reagiert wird. Darüber hinaus können und sollen Informationen über derartige Vorkommnisse der Vorbeugung künftiger Schadensereignisse dienen.

16.1.1 Überlegungen zu Informationssicherheitsereignissen

Informationssicherheitsereignisse, die im Rahmen des Sicherheitsmanagements einer besonderen Behandlung bedürfen, sind solche, die das Potenzial für große Schäden besitzen. Diese liegen somit in der Verantwortung des Informationssicherheitsmanagements. Sicherheitsprobleme, die nur lokal begrenzte und geringfügige Schäden verursachen oder verursachen können, sollten auch in der

lokalen Verantwortlichkeit gelöst werden. Das entlastet das Sicherheitsmanagement und ist wegen der Nähe zum Problem meist effizienter. Unbeschadet dessen sollten in der Nachbearbeitung („Lessons learned“) auch begrenzte Sicherheitsprobleme inklusive ihrer Lösung dokumentiert werden. Die Behandlung von Sicherheitsvorfällen verfolgt als Teil des Informationssicherheitsmanagements dabei folgende Ziele:

- Reaktionsfähigkeit, damit Sicherheitsvorfälle und Sicherheitsprobleme rechtzeitig bemerkt und an eine zuständige Stelle gemeldet werden,
- Entscheidungsfähigkeit, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall handelt,
- Handlungsfähigkeit, damit bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen und umgesetzt werden,
- Schadensminimierung, in dem weitere potenziell betroffene Bereiche rechtzeitig benachrichtigt werden und
- Effektivität, in dem die Fähigkeit zur Behandlung von Informationssicherheitsereignissen bzw. Sicherheitsvorfällen geübt und überwacht wird.

Um diese Ziele erreichen zu können, müssen zur Behandlung von Informationssicherheitsereignissen geeignete Vorgehensweisen sowie Organisationsstrukturen geplant und aufgebaut werden, also sinnvolle und erprobte Prozesse zum Umgang damit einzurichten. Die unterschiedlichen Arten solcher Ereignisse und die zugehörigen Abläufe und Regeln für die verschiedenen sollten klar definiert sein. Zwingende Voraussetzung dafür ist, dass das Management beteiligt ist und schließlich die Verfahren zur Behandlung von Informationssicherheitsereignissen in Kraft setzt.

Die Behandlung von Informationssicherheitsereignissen stellt auch einen wichtigen Teil des Sicherheitsmanagements dar und sollte daher auch im Sicherheitskonzept der Organisation beschrieben werden. So ist vor allem festzulegen, dass Sicherheitsvorfälle und Sicherheitsprobleme von den BenutzerInnen bzw. Betroffenen über die jeweils festgelegten Meldewege gemeldet werden. Weiters sind die Entscheidungsfindungswege zu beschreiben.

Die Behandlung von Sicherheitsvorfällen muss außerdem mit dem Notfallmanagement (siehe 17 Disaster Recovery und Business Continuity) abgestimmt werden, da es hier einerseits ähnliche Vorgehensweisen gibt, andererseits sich ein Sicherheitsvorfall zu einem Notfall entwickeln kann und es dann auf reibungsfreie Zusammenarbeit unter erschwerten Bedingungen ankommt. Dafür erweisen sich vertrauenswürdige informelle Kontakte als zweckmäßig, wenn sie rechtzeitig etabliert und laufend gepflegt werden. Nicht zuletzt ist die rasche und zuverlässige Behebung von Informationssicherheitsereignissen auch eine Frage, ob und inwieweit die MitarbeiterInnen hinsichtlich der Notwendigkeit für Sicherheitsmaßnahmen motiviert sind.

[Quelle: BSI M 6.58]

16.1.2 Festlegung von Verantwortlichkeiten bei Informationssicherheitsereignissen

Zur Behandlung von Informationssicherheitsereignissen sind geeignete Organisationsstrukturen erforderlich. Abhängig von der Art der Organisation, aber auch des Ereignisses müssen ggf. jeweils andere Personengruppen aktiv werden. Um sie vorab identifizieren zu können, empfehlen sich Planspiele, bei denen imaginäre Sicherheitsvorfälle durchgegangen werden und sich zeigt, welche Akteure in den verschiedenen zeitlichen Phasen benötigt werden. Jedenfalls sind für die handelnden Personengruppen Aufgaben, Kompetenzen sowie Art ihrer Benachrichtigung und Verpflichtung festzulegen.

Beispielhaft ist dies für die folgenden Gruppen angeführt:

- BenutzerInnen:
  Sobald sie eine sicherheitsrelevante Unregelmäßigkeit bemerken, müssen sie die entsprechenden Verhaltensregeln einhalten und den Sachverhalt über den vorgesehenen Meldeweg melden. Dazu muss schriftlich eine Verpflichtung zur Meldung geregelt und den BenutzerInnen klare, verständliche Verhaltensanweisungen übermittelt worden sein.
- AdministratorInnen:
  Sie haben Meldungen über sicherheitsrelevante Unregelmäßigkeiten, die mit den von ihnen betreuten IT-Systemen verbunden sind, entgegenzunehmen. Anschließend entscheiden sie, ob sie sie selbst beheben können oder ob sie die nächst höhere Eskalationsebene zu unterrichten haben. Derartige Entscheidungskompetenzen sollten in der Stellenbeschreibung sowie den Richtlinien zur Behandlung von Sicherheitsvorfällen festgelegt werden.
- Management:
  Wird bei schwerwiegenden Sicherheitsvorfällen unterrichtet und muss ggf. rasch Entscheidungen treffen. Jedenfalls trägt das Management auch in Krisen die Gesamtverantwortung, kann aber Teilverantwortungen delegieren. Besteht der Verdacht auf kriminelle Handlungen, schaltet das Management Polizei und Strafverfolgungsbehörden ein. In der Konzeption und Planung muss das Management den entsprechend festgelegten Vorgehensweisen zustimmen und sich seiner Rolle bei der Behandlung von Sicherheitsvorfällen bewusst sein.
- CISO:
  Nimmt Meldungen über Sicherheitsvorfälle, aber auch Informationssicherheitsereignisse entgegen, untersucht und bewertet die Ereignisse. Ein wesentliches Ergebnis dieser Bewertung ist die Entscheidung, ob ein Informationssicherheitsereignis zum Sicherheitsvorfall eskaliert wird und welche notwendigen Maßnahmen dann ergriffen bzw. veranlasst werden.

Dafür kann es mitunter sinnvoll sein, dem/der CISO begrenzte Ressourcen zur selbstständigen Behebung von Sicherheitsvorfällen zur Verfügung zu stellen. Jedenfalls ist es seine/ihre Aufgabe, ab einer bestimmten Schwere das Management zu informieren. In der Konzeption und Planung erarbeitet er/sie die Vorgehensweisen und Richtlinien zur Behandlung von Sicherheitsvorfällen und Informationssicherheitsereignissen. Notwendig ist dazu eine klar definierte Kompetenz- und Befugnisregelung für die CISOs.

Weitere Kompetenzen, sofern in der Organisation vorhanden:

- Helpdesk:
  Nimmt alle Störungsmeldungen entgegen und bewertet diese auch danach, ob ein Sicherheitsvorfall vorliegt. Besteht ein Verdacht, wird der/die CISO informiert. Damit die MitarbeiterInnen des Helpdesks solche Bewertungen durchführen können, sollten sie entsprechend geschult sein und Zugriff auf dokumentierte Auslöser und Anzeichen vergangener Sicherheitsvorfälle haben.
- Change Management:
  Mit Change Management befasste MitarbeiterInnen nehmen IT-Änderungsanträge (IT Change Requests) entgegen, welche bei Sicherheitsvorfällen die notwendigen Maßnahmen zur Schließung der Sicherheitslücken enthalten. Sie haben sicherzustellen, dass die notwendigen Maßnahmen schnell, effizient und ohne Auswirkungen auf die Qualität der IT-Services umgesetzt werden. Dazu sollte in den Richtlinien zur Behandlung von Sicherheitsvorfällen festgelegt werden, dass Änderungen zur deren Behebung als dringlich (Emergency Changes) zu behandeln sind und dementsprechend priorisiert im Change Management Prozess behandelt werden.
- Revision, Informationssicherheitsmanagementsystem:
  Der Revision kann die Aufgabe übertragen werden, in regelmäßigen Abständen die Wirksamkeit des Managementsystems für Sicherheitsvorfälle zu prüfen. Weiters kann sie beauftragt werden, bei der Nachbereitung von Sicherheitsvorfällen mitzuwirken und Prüfungen durchzuführen. Dies sollte in den Richtlinien zur Behandlung von Sicherheitsvorfällen festgelegt werden.
- Öffentlichkeitsarbeit / Pressestelle:
  Bei schwerwiegenden Sicherheitsvorfällen mit entsprechendem Medieninteresse sollte die Information der Öffentlichkeit ausschließlich durch die Pressestelle bzw. im Umgang mit Medien geschulte MitarbeiterInnen für Öffentlichkeitsarbeit erfolgen. Muss ein Sprecher des Managements an die Öffentlichkeit treten, muss die Pressestelle für geeignetes Briefing sorgen. Dabei sollte der Vorfall nicht beschönigt oder verharmlost, sondern sachlich dargestellt werden. Gegenteilige Informationen oder unterschiedliche, widersprüchliche Aussagen führen zu noch mehr öffentlichem Interesse und Imageverlust. Die Pressestelle muss Informationen über den Sicherheitsvorfall zusammen mit den technischen Experten aufbereiten und mit dem Management abstimmen. Auch dies ist in den Richtlinien zur Behandlung von Sicherheitsvorfällen festzulegen.
- Expertenteam für Sicherheitsvorfälle:

Bei schwierigen oder schwerwiegenden Sicherheitsvorfällen kann es nötig sein, ein Expertenteam (CSIRT - Computer Security Incident Response Team) zusammenzustellen, um system- oder standortspezifische Erkennungs-, Sicherstellungs-, Analyse- und Reaktionshandlungen vorzunehmen. Seine Mitglieder müssen dazu Zugriff auf die verdächtigen Systeme und Zutritt zu den betroffenen Standorten sowie Befugnisse zur eigenverantwortlichen Durchführung der Aufgaben bekommen. Sie handeln jedenfalls strikt nach den Richtlinien für die Behandlung von Sicherheitsvorfällen und den Anweisungen des Managements und des/der CISO. Informationen über den jeweiligen Sicherheitsvorfall erfolgen über den/die CISO.

- Sicherheitsvorfall-Team:
  In großen Organisationen kann sinnvollerweise ein koordinierendes Sicherheitsvorfall-Team benannt werden. Es setzt sich aus Vertretern unterschiedlicher Organisationsbereiche wie z. B. Management, CISO, Datenschutzbeauftragte, IT-LeiterIn, Revision, Pressestelle, Beschaffung, Haustechnik u. s. w. zusammen und soll bei schwerwiegenden Sicherheitsvorfällen rasche strategische Entscheidungen - auch ggf. für improvisierte Maßnahmen - treffen können. Daher sind seine Mitglieder sowie der/die LeiterIn namentlich zu benennen und die Kontaktdaten an geeigneten Stellen zu hinterlegen. Das Team tritt nur bei konkreten Sicherheitsvorfällen zusammen, seine Kompetenzen müssen vorab schriftlich festgehalten und vom Management genehmigt sein.

[Quelle: BSI M 6.59, DER.2.1]

16.1.3 Erstellung eines Incident Handling-Plans und Richtlinien zur Behandlung von Sicherheitsvorfällen

Viele Sicherheitsvorfälle werden erst durch falsche oder planlose Reaktionen zu einem größeren Problem, wenn in der Stresssituation überhastet Entscheidungen getroffen oder falsche Maßnahmen gesetzt werden. Detaillierte Vorgaben in Form eines Incident Handling-Planes (IHP) sowie zielgruppenorientierte Richtlinien für die Behandlung von Sicherheitsvorfällen, die den jeweiligen MitarbeiterInnen bekannt gemacht werden, ermöglichen allen Beteiligten sich in Ausnahmesituationen richtig zu verhalten sowie ruhig und besonnen zu handeln.

Incindent Handling Plan

Der IHP ist das zentrale Dokument und legt in schriftlicher Form und verbindlich fest:

- wie ein Sicherheitsvorfall bzw. sicherheitsrelevantes Ereignisses definiert ist,
- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- Verantwortlichkeiten für die Meldung bzw. Untersuchung sicherheitsrelevanter Vorfälle,

- die einzuhaltenden Meldewege,
- ob und in welcher Form schadensbehebende oder schadensvorbeugende Maßnahmen zu ergreifen sind und die Verantwortlichkeiten dafür,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw. Gegenmaßnahmen treffen müssen.

Darüber hinaus muss auch geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es ist dafür Sorge zu tragen, dass evtl. mitbetroffene Stellen schnellstens informiert werden.

Es sollte auch geklärt sein, wie mit der im Rahmen von Sicherheitsvorfällen anfallenden Mehrarbeit umzugehen ist, also ob die Arbeitszeitregelungen der Behörde bzw. des Unternehmens um Ausnahmeregelungen für Mehrarbeit, Wochenendarbeit etc. bei Sicherheitsvorfällen erweitert werden muss. Darüber hinaus ist auch sicherzustellen, dass dann bei Bedarf auch die Diensträume außerhalb der regulären Arbeitszeit genutzt werden können.

Richtlinien zur Behandlung von Sicherheitsvorfällen bzw. sicherheitsrelevanten Ereignissen

sind jeweils zielgruppenorientierte Verhaltens- und Handlungsanweisungen für die im Fall von Sicherheitsproblemen befassten bzw. betroffenen MitarbeiterInnen. Bei ihrer Erstellung sollte darauf geachtet werden, dass sie jeweils vollständig und praktisch anwendbar sind, insbesondere dass die Aufgaben aller Beteiligten klar formuliert und allfällige Ausnahmefälle inkl. deren Genehmigungsverfahren dokumentiert sind. AdministratorInnen, Wartungspersonal etc. benötigen zusätzliche technische Handlungsanweisungen. Selbstverständlich müssen alle Richtlinien mit dem Managementsystem zur Sicherheitsvorfallsbehandlung konform sein.

Es gibt dabei allgemein gültige Verhaltensregeln, die für sämtliche vorstellbaren Sicherheitsvorfälle gelten, im Unterschied zu IT-spezifischen. Als allgemein gültige Verhaltensregeln für alle Arten von sicherheitsrelevanten Unregelmäßigkeiten können festgehalten werden:

- Ruhe bewahren und keine übereilten Maßnahmen ergreifen.
- Unverzügliche Meldung an die im Melde- bzw. Alarmierungsplan vorgesehenen Stellen.
- Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden.
- Erste, auf persönlichen Erfahrungen beruhende Einschätzung der möglichen Schadenshöhe, Folgeschäden, intern und extern Betroffenen sowie möglicher Konsequenzen an die vorgesehene Stelle bzw. Vorgesetzten.

- Alle Begleitumstände sind durch die Betroffenen klar, offen und ungeschönt zu erläutern.
- Informationen über den Sicherheitsvorfall dürfen nicht unautorisiert an Dritte weitergegeben werden.

Darüber hinaus können spezifische Verhaltensregeln insbesondere an diejenigen Betroffenen ausgegeben werden, die als Meldestellen für Sicherheitsvorfälle fungieren und die ersten Entscheidungen fällen bzw. die ersten Maßnahmen ergreifen sollen. Dazu gehören AdministratorInnen, IT-Anwendungsverantwortliche und Sicherheitsbeauftragte, beispielsweise im Fall von:

- Auftreten von Schadprogrammen,
- Verlust der System-, Netz- oder Datenintegrität,
- Sicherheitsvorfällen im WLAN.

Solche Richtlinien sollten auch in Papierform greifbar sein, da elektronische Formen vom Sicherheitsvorfall betroffen sein könnten.

Sie sind bei jeder relevanten Änderung in der Organisation, den Geschäftsprozessen oder der IT umgehend zu aktualisieren, damit die Verhaltensregeln noch greifen und die Meldewege korrekt bleiben.

16.1.4 Prioritäten bei der Behandlung von Sicherheitsvorfällen

Da ein Sicherheitsvorfall erfahrungsgemäß oft durch eine Verkettung verschiedener Ursachen entsteht und unterschiedliche Geschäftsprozesse, Anwendungen und IT-Systeme gleichzeitig betrifft, ist es wichtig, die Prioritäten für die Problembeseitigung möglichst vorab festzulegen. Davon hängt unter anderem ab, in welcher Reihenfolge die Behebung begonnen wird und ihr Ressourcen zugeordnet werden.

Die Prioritätensetzung orientiert sich an der Art des Vorfalls und den Gegebenheiten der betroffenen Organisationen. Dabei erweisen sich die Erkenntnisse einer vorab durchgeführten Risikoanalyse als hilfreich, wenn dabei auch die für die Organisation relevanten Schadensszenarien **kategorisiert** wurden, wie etwa:

- Verstoß gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des Rechts, selbst über die Preisgabe und Verwendung von personenbezogenen Daten zu bestimmen.
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Außenwirkung,
- finanzielle Auswirkungen.

In jeder einzelnen dieser Kategorien können tolerierbare, erhebliche oder existenzbedrohende Schäden drohen, demnach gibt es dafür jeweils normalen, hohen oder sehr hohen **Schutzbedarf** für die zugrunde liegenden Informationen und Geschäftsprozesse. Die Schwierigkeit bei der Analyse liegt in der Bewertung, was etwa tolerable oder erhebliche Schäden sind. Ist dies durchgeführt, wird jeder Kombination von Schadensszenario und Schutzbedarfshöhe eine Priorität zugeordnet, vom Management genehmigt und allen Entscheidungsträgern bei der Behandlung von Sicherheitsvorfällen bekannt gegeben. Höchste Priorität hat demnach der Geschäftsprozess mit dem höchsten Schutzbedarf in den meisten Kategorien.

Tritt ein Sicherheitsvorfall ein, so können nach dessen Bewertung die zu erwartenden Schäden eingeschätzt und den bekannten Schadensszenarien zugeordnet werden. Anschließend werden diese Schäden für die betroffenen Geschäftsprozesse in die Klassen „normal“, „hoch“ und „sehr hoch“ eingeteilt und damit dann über die Priorität und Reihenfolge ihrer Behebung entschieden. Eine solche Vorab-Prioritätensetzung kann nur eine erste Orientierung bieten - im individuellen Ernstfall muss sie ggf. angepasst werden.

[Quelle: BSI M 6.62]

16.1.5 Meldewege bei Sicherheitsvorfällen

Bei Sicherheitsvorfällen ist es eine Pflicht, alle davon betroffenen Stellen so schnell wie möglich zu informieren. Dazu sind vorab entsprechende Meldewege zu definieren.

Betroffene sind vor allem diejenigen Stellen, die durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen, Informationen darüber aufbereiten oder bei der Vorbeugung oder Behebung helfen können. Wenn erforderlich, sollte auch die Öffentlichkeit aufgeklärt werden, insbesondere wenn schon Informationen durchgesickert sind. Dafür sollte es ein klares Konzept geben, wer durch wen in welcher Reihenfolge in welcher Tiefe informiert wird. Weiters muss sichergestellt sein, dass Auskünfte über den Sicherheitsvorfall ausschließlich durch benannte Verantwortliche, wie zum Beispiel das Sicherheitsmanagement oder eine Pressestelle, gegeben werden. Das ist nicht nur wegen potenzieller Imageschäden, sondern ggf. auch rechtlich relevant. Falsche oder schöngefärbte Informationen können zu Verwirrung, Fehleinschätzungen, Imageverlust und erst recht gewecktem öffentlichen Interesse führen.

- Interne Stellen (LeiterIn der IT, LeiterIn betroffener Fachabteilungen, BenutzerInnen, AdministratorInnen, CISO, Datenschutzbeauftragte, Helpdesk, Change Management, Haustechnik, Portier, Wachpersonal):

Solange noch nicht klar ist, ob ein Sicherheitsvorfall vorliegt oder wie schwerwiegend er ist, sollten die potenziell betroffenen internen Kräfte gebeten werden, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen. Sind die erforderlichen Gegenmaßnahmen bei einem Sicherheitsvorfall bekannt, müssen die betroffenen internen Stellen kurzfristig darüber informiert werden, was sie tun müssen, um die Auswirkungen eines Sicherheitsvorfalls zu minimieren oder um den sicheren Zustand wiederherzustellen.

- Externe Stellen (Kunden, Lieferanten, freie MitarbeiterInnen, Subunternehmen, ggf. auch IT-Service- oder Softwaredienstleister, Netzbetreiber):
  Falls der Sicherheitsvorfall nicht intern begrenzt ist, sollten alle externen Stellen, die ebenfalls betroffen sind oder sein können, über das aufgetretene Sicherheitsproblem und notwendige Gegenmaßnahmen informiert werden, sowie darüber, wie die Auswirkungen eingedämmt werden können. Erfolgt das nicht oder zu spät, kann die weitere Zusammenarbeit bzw. das bestehende Vertrauensverhältnis nachhaltig beeinträchtigt werden. Bei manchen Vorfällen muss auch die Polizei bzw. ein Rechtsbeistand beigezogen werden.
- Öffentlichkeit, Medien:
  Bei größeren oder komplexeren Sicherheitsvorfällen kann es notwendig sein, die Öffentlichkeit aufzuklären. Alle Pressekontakte sollten hierbei ausschließlich über befugte SprecherInnen laufen. Diese müssen über den Sicherheitsvorfall, über Schadenshöhe, erforderliche Gegenmaßnahmen und über benachrichtigte Stellen ausreichend informiert sein. Derartige Informationen für die Öffentlichkeit bergen immer die Gefahr, dass Nachahmer animiert werden und dürfen daher nicht zu konkret sein. Weiters ist bei allen Personen, die Informationen über Sicherheitsvorfälle einholen wollen, deren Identität zu überprüfen, damit sich die Angreifer nicht über den Erfolg ihrer Attacke auf dem Laufenden halten können.
- Sicherheitsgemeinde (Community):
  Liegt dem Sicherheitsvorfall eine bisher noch nicht bekannte Sicherheitslücke zugrunde, sollten weitere Stellen informiert werden, damit davor gewarnt wird und Gegenmaßnahmen entwickelt werden können, wie etwa:
  - Hersteller von Virenschutzprogrammen,
  - Hersteller des Betriebssystems oder der Applikationssoftware, wenn die Sicherheitslücke darin aufgetreten ist,
  - externes Computer Emergency Response Team (CERT), wenn der Sicherheitsvorfall auf system- oder applikationsspezifischen Sicherheitslücken beruht.

Die Priorität hängt dabei vom Vorfall ab:

- Bei äußeren Ereignissen wie Feuer, Wasser, Stromausfall, Einbruch und Diebstahl sind die örtlich verfügbaren Einsatzkräfte sowie die technische Einsatzleitung zu unterrichten (Feuerwehr, Haustechnik, Portierdienst, Wachdienst, …).

- Bei hardwaretechnischen Problemen oder bei Unregelmäßigkeiten bei Betrieb der IT-Systeme sind die zuständigen AdministratorInnen bzw. der Helpdesk/ Benutzer-Support zu benachrichtigen.
- Bei großflächigen Ausfällen oder sonstigen im Notfallhandbuch aufgeführten Szenarien ist der Notfallbeauftragte und Leiter des Krisenstabs zu informieren.
- Bei vermuteten vorsätzlichen Handlungen und bei ansonsten nicht zuzuordnenden Ereignissen (z. B. Datenmanipulationen, unerlaubter Ausübung von Rechten, Spionage- und Sabotageverdacht) ist der/die CISO bzw. das Sicherheitsmanagement zu benachrichtigen.
- Existiert eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen sollte diese Stelle jedenfalls mit informiert werden, damit dort der Sicherheitsvorfall dokumentiert werden kann und bei Bedarf weitere Meldungen zugeordnet werden können.

Allen MitarbeiterInnen müssen die AnsprechpartnerInnen und die Meldewege für alle Arten von Sicherheitsvorfällen bekannt sein, etwa als Liste im internen Telefonverzeichnis oder im Intranet mit Namen, Telefonnummern und E-Mail-Adressen der jeweiligen AnsprechpartnerInnen. Eine solche Liste sollte auch in Papierform vorhanden sein, falls die IT vom Vorfall betroffen ist.
Es muss einfach und rasch möglich sein, Verdachtsfälle weiterzumelden. Authentizität der KommunikationspartnerInnen und die Vertraulichkeit der über den Verdachtsfall gemeldeten Informationen sind sicherzustellen. Auskünfte über einen Sicherheitsvorfall dürfen gegenüber Dritten nur durch autorisierte Personen gegeben werden.

Das Funktionieren der Meldungen sollte auch immer wieder durch Übungen überprüft werden.

[Quelle: BSI M 6.60, M 6.65]

16.1.6 Behebung von Sicherheitsvorfällen

Im Rahmen des Incident Managements wird bei der Störungsbehebung geprüft, ob eine ähnliche Störung bereits aufgetreten und dafür eine geeignete Lösung vorhanden ist, beispielsweise indem die Fehlerursache behoben wird oder nur ein Workaround zur Beseitigung der Symptome gefunden wird. Damit die Störung unterschiedlichen Support-Ebenen entsprechend ihrem fachlichen Wissen zur Analyse und Diagnose zugewiesen werden kann, müssen die Rollen und Verantwortlichkeiten sowie der Informationsfluss bereits im Vorfeld etabliert worden sein.

Im Zuge eines Review des Vorfalls werden betrachtet:

- Erfasste Probleme
- Bekannte Fehler (Known Errors)

- Geplante bzw. durchgeführte Änderungen in IT-Komponenten

Wird ein Workaround gefunden, so müssen umgehend die erforderlichen Umsetzungsmaßnahmen eingeleitet werden. Der Workaround versetzt die BenutzerInnen in die Lage, den gestörten Service mindestens in eingeschränkter Form wieder zu nutzen (Wiederanlauf in den eingeschränkten Betrieb). Zusätzlich wird dadurch die Wirkung der Störung auf die Geschäftsprozesse minimiert und mehr Zeit zur Bereitstellung einer endgültigen Lösung gewonnen.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert worden ist, sollten die erforderlichen Maßnahmen zu dessen Behebung ausgewählt und umgesetzt werden. Dazu muss zunächst das Problem eingegrenzt und beseitigt werden und anschließend der „normale“ Zustand wiederhergestellt werden.

Eine Voraussetzung für die Untersuchung und Beseitigung einer Sicherheitslücke ist das entsprechende Fachwissen. Daher muss das Personal entsprechend geschult sein oder es müssen ExpertInnen zu Rate gezogen werden. Dafür sollte eine Liste mit den Kontaktadressen von einschlägigen internen und externen ExpertInnen aus den verschiedenen Themenbereichen vorbereitet sein, damit diese schnell zu Rate gezogen werden können. Zu den externen ExpertInnen gehören unter anderem

- Hersteller bzw. Vertreiber der betroffenen IT-Systeme,
- Hersteller bzw. Vertreiber der eingesetzten Sicherheitssysteme, wie Computervirenschutzprogramm, Firewall, Zutrittskontrolle etc.,
- externe BeraterInnen mit sicherheitsspezifischem Fachwissen und
- Computer Emergency Response Teams (CERTs).

Für die Kommunikation mit externen ExpertInnen muss vorab ein sicheres Verfahren definiert und eingerichtet werden.

Reaktion auf fahrlässige oder vorsätzliche Handlungen

Bei Sicherheitsvorfällen, die durch AngreiferInnen ausgelöst wurden, muss entschieden werden, ob der entdeckte Angriff weiter beobachtet oder möglichst schnell Gegenmaßnahmen durchgeführt werden sollen. Damit kann versucht werden, die AngreiferInnen auf frischer Tat zu ertappen, aber dies birgt auch das Risiko, dass die AngreiferInnen in der Zwischenzeit Daten zerstören, manipulieren oder auslesen.

Leider werden Sicherheitsproblemen häufig auch von eigenen MitarbeiterInnen verursacht, sei es durch Versehen, fehlerhafte Arbeitsabläufe, aber auch durch Nichtbeachtung von Sicherheitsmaßnahmen oder gar vorsätzliche Handlungen. Daher muss bei allen intern verursachten Sicherheitsproblemen der Auslöser untersucht werden. In vielen Fällen wird sich zeigen, dass die Probleme aus fehlerhaften oder missverständlichen Regelungen resultieren. Dann müssen die Regelungen entsprechend geändert oder um weitere, z. B. technische Maßnahmen, ergänzt werden.

Sind Sicherheitsprobleme vorsätzlich oder aus Nachlässigkeit verursacht worden, sollten angemessene Konsequenzen erfolgen.

[Quelle: BSI M 6.64]

16.1.7 Eskalation von Sicherheitsvorfällen

Nach der Regelung der Verantwortlichkeiten für Sicherheitsvorfälle sowie Bekanntgabe der Verhaltensregeln und Meldewege an alle Betroffenen, muss auch eine Eskalationsstrategie formuliert werden, welche regelt, wie mit eingegangenen Meldungen weiter verfahren wird.

Eine solche Eskalationsstrategie sollte zwischen den Verantwortlichen für Störungs- und Fehlerbehebung (Incident Management) und dem Informationssicherheitsmanagement abgestimmt werden. Dadurch können eventuell bereits vorhandene Methoden und Verfahren effektiv und effizient mitgenutzt werden.

Diejenigen, die eine Meldung über einen Sicherheitsvorfall erhalten haben, müssen diesen zunächst untersuchen und bewerten. Falls es sich tatsächlich um einen Sicherheitsvorfall handelt, müssen weitere Maßnahmen ergriffen werden. Dabei stellen sich folgende Fragen:

- Wer ist im Fall einer Eskalation, also der Ausweitung der Aktionskette, zu unterrichten?
- In welchen Fällen ist eine sofortige Eskalation vorzunehmen?
- Unter welchen Umständen ist ansonsten eine Eskalation durchzuführen und wann wird diese vorgenommen (sofort, am nächsten Tag, am nächsten Werktag)?
- Über welche Kanäle bzw. Medien wird die Meldung weitergegeben?

Die Antworten zu diesen Fragen sind in der Eskalationsstrategie festzuhalten und bekannt zu geben.

Damit tatsächliche sicherheitsrelevante Ereignisse ohne Zeitverlust nach ihrer Kenntnisnahme von den Verantwortlichen bearbeitet werden können, sind im Vorfeld Eskalationsstrategien, -ansprechpartnerInnen und -wege zu definieren. Empfehlenswert ist dazu die Einrichtung von Schnittstellen zu den Eskalationsverfahren der Verantwortlichen für Störungs- und Fehlerbehebung (Incident Management), sowie dem Notfallmanagement zur Synchronisierung. Grundsätzlich sind zwei Eskalationstypen möglich:

- Die **fachliche Eskalation** bei der Störungs- und Fehlerbehebung wird eingeleitet, wenn für die Erstlösung im First Level Support keine zutreffende Lösung, z. B. in Form einer Checkliste, vorliegt oder das Szenario im Eskalationsweg etwa die Einbeziehung weiterer notwendiger KompetenzträgerInnen vorsieht. Das Sicherheitsmanagement sollte regelmäßig

nach den gleichen Bedingungen einbezogen werden. Insbesondere bei vermuteten Sicherheitsvorfällen, für die im First Level Support kein „Matching Szenario“ vorliegt, sollte sofort in Richtung Sicherheitsmanagement eskaliert werden. Dem First Level Support sollte daher die aktuelle Eskalationsstrategie vorliegen.

- Die **hierarchische Eskalation** sollte eingeleitet werden, wenn neben den oben genannten Voraussetzungen absehbar ist, dass vereinbarte Wiederherstellungszeiten nicht eingehalten werden können oder aber im Verlauf der Bearbeitung Entscheidungen getroffen werden müssen, die nicht in der Kompetenz der BearbeiterInnen liegen, z. B. weil
  - sicherheitskritische Geschäftsprozesse betroffen sind,
  - existenzbedrohende Schäden vermutet werden,
  - kriminelle Handlungen vermutet werden,
  - folgenreiche Flächenstörungen oder Notfälle abzusehen sind etc.

Es ist erforderlich, dass für die Planung der Eskalationsstrategie ebenfalls die erwarteten Reaktionen und Aktivitäten der Eskalationsinstanz klar definiert werden und die Eskalation nicht nur einen informativen Charakter erhält. Alle durchgeführten Eskalationen sind nachvollziehbar zu dokumentieren. Die Eskalationsstrategie kann in drei Schritten erstellt werden:

Schritt 1: Festlegung der Eskalationswege

Wer für die Behandlung von Sicherheitsvorfällen verantwortlich ist, wurde in 16.1.2 Festlegung von Verantwortlichkeiten bei Informationssicherheitsereignissen festgelegt. In der Festlegung des Eskalationsweges ist zu definieren, wer an wen eine Meldung weitergibt. Dies lässt sich in einfacher Weise durch eine Grafik darstellen. Dabei sollten sowohl die regulären Eskalationswege als auch der Vertretungsfall berücksichtigt werden.

Schritt 2: Entscheidungshilfe für Eskalation

Es wird zunächst festgelegt, in welchen Fällen eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen durchgeführt werden sollte. Ein Beispiel für eine tabellarische Aufstellung ist:

Ereignis	Sofort zu informieren
Infektion mit einem Computervirus	CISO, AdministratorInnen
Brand	Portiere, Brandschutzbeauftragte, Feuerwehr
Vorsätzliche/vermutete kriminelle Handlungen	CISO
Verdacht auf Werksspionage	CISO, Management

Ereignis	Sofort zu informieren
Notwendigkeit, Polizei und Strafverfolgungsbehörden einzuschalten	Management
Existenzbedrohende Schäden	Management, Notfallbeauftragte, LeiterIn des Krisenstabs

Tabelle 16.1: Beispiele für Eskalation

Anschließend ist für die restlichen Fälle vorzugeben, wann eine Eskalation stattzufinden hat. Gründe dafür können sein:

- Die zu erwartende Schadenshöhe übertrifft den Verantwortungsbereich der Stelle, die die Meldung entgegengenommen hat.
- Die Kosten und Ressourcen für die Schadensregulierung übertreffen deren Kompetenzbereich.
- Die Komplexität des Sicherheitsvorfalls übersteigt deren Kompetenz- bzw. Zuständigkeitsbereich.

Schritt 3: Art und Weise der Eskalation

Festgelegt wird, auf welche Weise die jeweils nächste Stelle in der Eskalationskette unterrichtet werden soll, etwa:

- persönliche Vorsprache
- schriftlicher Bericht
- E-Mail
- Telefon, Handy
- Trouble Ticket System (Issue-Tracking-System; das ist eine Softwarelösung zum Empfang, Bestätigung, Bewertung und Bearbeitung von Anfragen (Tickets; das sind eingehende Kundenanrufe, E-Mails etc.). Solche Systeme weisen einer definierten verantwortlichen Stelle ein Ticket zur Bearbeitung zu - ist das Problem gelöst, hat man ein „closed ticket“. Damit geht keine Anfrage verloren und man hat jederzeit einen Überblick über die behandelten Vorgänge)
- Bote mit verschlossenem Umschlag

Werden für die Eskalation Werkzeuge wie z. B. Ticket-Systeme verwendet, müssen diese darauf geprüft werden, dass sie auch während eines Sicherheitsvorfalls oder Notfalls zur Verfügung stehen und damit auch vertrauliche Informationen verarbeitet werden können.

Ebenso ist festzulegen, wann diese Meldung weitergegeben wird, etwa:

- bei Ereignissen, die Sofortmaßnahmen erfordern, z. B. einer telefonischen Bombendrohung: unverzüglich.
- bei Ereignissen, die eine zügige Bearbeitung erfordern, z. B. Anzeichen auf eine Infektion mit einem Computervirus im LAN: sofort innerhalb einer Stunde.

- bei Ereignissen, die zwar beherrscht werden, aber einer Unterrichtung der nächsten Eskalationsstufe erfordern, z. B. Angriffe mit Schadsoftware, die aber bekannt sind und erfolgreich am Sicherheitsgateway blockiert werden: am nächsten Werktag.

Bei der Festlegung der Kriterien für die Weitergabe der Meldungen sollten auch die Definitionen der fachlichen und hierarchischen Eskalation (siehe oben) berücksichtigt werden.

Eine solche Eskalationsstrategie sollten alle möglichen EmpfängerInnen von Meldungen über Sicherheitsvorfälle erhalten, um zügige Reaktionen zu ermöglichen. Die Eskalationsstrategie und die Meldewege müssen in Übungen erprobt werden, damit auch bei den Beteiligten die notwendige Routine zur Verringerung von Stress in Krisensituationen erreicht wird. Da sich Meldewege und Einschätzungen von Ereignissen immer wieder ändern können, muss die Eskalationsstrategie regelmäßig (z. B. mindestens einmal jährlich) überprüft und aktualisiert werden.

Zur Eindämmung eines Sicherheitsvorfalls ist i. Allg. kurzfristiges Handeln erforderlich. Das heißt, dass eventuell MitarbeiterInnen aus anderen Projekten abgerufen oder auch außerhalb der Arbeitszeit herangezogen werden müssen. Daher müssen auch anfallende Mehrarbeit und Rufbereitschaft geregelt sein.

[Quelle: BSI M 6.66]

16.1.8 Nachbereitung von Sicherheitsvorfällen (Lessons Learned)

Aus jedem Sicherheitsvorfall kann man etwas lernen. Um aus einem eingetretenen Sicherheitsvorfall den maximalen Lerneffekt ziehen zu können, darf die Nachbereitung nicht vernachlässigt werden. Oftmals lassen sich daraus Verbesserungen im Umgang mit Sicherheitsvorfällen herausarbeiten oder Rückschlüsse auf die Wirksamkeit des Sicherheitsmanagements bzw. der vorhandenen Sicherheitsmaßnahmen ziehen.

Dabei sind unter anderem folgende Aspekte zu beachten:

Reaktionszeit

Wie schnell wurde der Sicherheitsvorfall bemerkt und welche Informationen standen für die Bewertung zur Verfügung?

Sind technische Detektionsmaßnahmen nachzurüsten?

Wie lange dauerte es, bis die Meldung den erforderlichen Meldeweg durchlaufen hat?

Wie schnell erfolgten Entscheidungen über die zu treffenden Maßnahmen, wie lange dauerte deren Umsetzung und wann erfolgte die Benachrichtigung der betroffenen internen und externen Stellen?

War der Meldeweg jedem bekannt oder sind zusätzliche Sensibilisierungsmaßnahmen und Informationen notwendig?

Wirksamkeit der Eskalationsstrategie

Wurde die festgelegte Eskalationsstrategie eingehalten, welche zusätzlichen Informationen waren notwendig?

Muss die Eskalationsstrategie angepasst werden?

Effektivität der Untersuchung

War die Einschätzung der Schadenshöhe des Sicherheitsvorfalls korrekt?

Waren die berücksichtigten Prioritäten angemessen?

Wurde für die Untersuchung ein geeignetes Sicherheitsvorfall-Team eingesetzt?

Benachrichtigung betroffener Stellen

Wurden tatsächlich sämtliche betroffenen Stellen benachrichtigt, war die Benachrichtigung zeitlich ausreichend schnell?

Müssen ggf. schnellere Wege der Benachrichtigung gefunden werden?

Rückmeldung an meldende Stelle

Diejenigen Stellen, die einen Sicherheitsvorfall entdeckt und diesen weitergemeldet haben, sollten darüber informiert werden, wann der Sicherheitsvorfall erfolgreich behoben wurde, welche Schäden entstanden sind und welche Maßnahmen ergriffen wurden. Dies zeigt, dass solche Meldungen ernst genommen werden und fördert die Motivation - vor allem wenn damit ein entsprechendes Lob verbunden ist.

Tätermotivation

Stellt sich heraus, dass der Sicherheitsvorfall auf eine vorsätzliche Handlung zurückzuführen ist, sollte die Motivation der TäterInnen untersucht werden. Handelt es sich dabei um InnentäterInnen, kommt der Motivation eine besondere Bedeutung zu. Stellt sich heraus, dass die Ursache im Bereich des Betriebsklimas zu sehen ist, sollte dies auch der Managementebene bekanntgegeben werden, da zu befürchten ist, dass Fehl- bzw. vorsätzliche Handlungen wieder auftreten können.

Bericht

Das Management sollte mindestens einmal jährlich einen aufbereiteten Bericht über Anzahl, Ursachen und Auswirkungen von Sicherheitsvorfällen erhalten. Je nach Relevanz der Nachbereitungsergebnisse sollte das Management sofort unterrichtet werden, um Verbesserungen oder Aktionen zu veranlassen. Eine solche Nachbereitung sollte durch eine Organisationseinheit durchgeführt werden, die nicht Teil des Meldeplans ist.

Weiterentwicklung der Richtlinien

Es ist sinnvoll aus den Erfahrungen heraus die Richtlinien für den Umgang mit Sicherheitsvorfällen derart zu erweitern bzw. überarbeiten, wie bei Auftreten eines vergleichbaren Sicherheitsvorfalls zu verfahren ist. Da jetzt die Probleme real bearbeitet wurden, können Handlungsanweisungen effizienter ausgearbeitet werden als bei der Erstellung auf einer theoretischen Basis. Immerhin zeigt der aufgetretene Sicherheitsvorfall, dass ein Bedarf für eine Handlungsanweisung gegeben ist. Unter Umständen kann es sinnvoll sein, dann auch die Notfalldokumentation zu aktualisieren.

[Quelle: BSI M 6.66]

16.1.9 Computer Emergency Response Team (CERT)

Computer Emergency Response Teams (CERTs) oder auch CSIRTs sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten Advisories über aktuelle Schwachstellen in Hard- und Softwareprodukten und geben Empfehlungen zu deren Behebung. CERTs werden national bzw. von verschiedenen Organisationen oder Verbänden unterhalten und sind zunehmend international vernetzt.

Aufgaben von CERTs:

- Untersuchung der Ursachen und Auswirkungen von sicherheitsrelevanten Vorfällen,
- Aufzeichnung und Auswertung von Vorfällen inkl. Behebung,
- Hilfestellung bei der Behandlung von sicherheitsrelevanten Vorfällen durch Expertenwissen und zusammengetragene Erfahrungen.

Ob innerhalb einer Institution ein (oder evtl. auch mehrere) CERT(s) eingerichtet wird, hängt in erster Linie von der Größe dieser Institution und der erwarteten Anzahl und Schwere der Vorfälle ab. In kleineren Institutionen wird eine Behandlung und Aufzeichnung der sicherheitsrelevanten Vorfälle durch eine

in der IT-Sicherheitspolitik zu benennende Person - dies wird i. Allg. der/die Datenschutzbeauftragte oder CISO sein - angemessen sein, in großen oder besonders sicherheitssensiblen Institutionen ist die Einrichtung von CERTs zu empfehlen.

Organisationsübergreifende bzw. nationale CERTs ermöglichen, Daten über sicherheitsrelevante Vorfälle auf breiter Basis auszutauschen und bieten damit eine sehr wertvolle und nützliche Informationsquelle, etwa über die Häufigkeit des Eintretens von Bedrohungen, neuartige Angriffe und eine Summe an Erfahrungen, wie Vorfälle behoben werden konnten.

Wesentlich für das rasche Funktionieren von CERTs ist neben einer klaren formalen und immer aktuellen Dokumentation der Kommunikationswege eine möglichst gute informelle Kommunikation - je besser die Teammitglieder einander persönlich kennen, desto höher ist das Vertrauen - z. B. wenn im Fall schwerer Krisen die normalen Kommunikationswege ausgefallen sind und improvisierte Entscheidungen gemeinsam getroffen werden müssen.

GovCERT in Österreich

GovCERT.AT ist das „Government Computer Emergency Response Team“ für die öffentliche Verwaltung und die kritische Informationsinfrastruktur (KII) in Österreich.

Seit April 2008 betreibt das Bundeskanzleramt diese Einrichtung in Kooperation mit CERT.at zur Behandlung beziehungsweise Verhinderung von Sicherheitsvorfällen im Bereich der Informations- und Kommunikationstechnologien (IKT).

Die Rolle des nationalen CERT ist zunächst die einer Informationsdrehscheibe. Es koordiniert betreiberübergreifend die Antwort auf Sicherheitsvorfälle und berät kleine und mittlere Unternehmen. Es gibt Warnungen über kritische Schwachstellen und Sicherheitslücken in Software und Computernetzen heraus und bietet Tipps zur Vermeidung von Angriffen.

Auf nationaler Ebene erfüllt GovCERT allerdings auch eine Koordinationsfunktion zwischen den einzelnen Stellen der öffentlichen Verwaltung und den Betreibern kritischer Infrastruktur:

- Sammlung und Bewertung von Vorfällen aus dem operativen IKT-Betrieb der Bundes-, Landes-, Städte- und Gemeindeverwaltungen,
- Koordinierung von Gegenmaßnahmen,
- Beschaffung und Bewertung von Nachrichten aus öffentlich und nicht öffentlich zugänglichen Quellen

Zusätzlich zu den oben aufgelisteten Aufgaben bietet GovCERT Öffentlichkeitsarbeit und Beratung zur Sensibilisierung bezüglich des Themas Sicherheit im Internet und IKT-Betrieb. Es nutzt dazu die technischen Ressourcen und die technische Qualifikation von CERT.at (siehe unten) für die Behandlung sicherheitsrelevanter Vorfälle.

Internationale Kooperation

GovCERT ist die österreichische Kontaktstelle für ausländische Regierungen und internationale Organisationen zu Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische Interessenten weiter. In dieser Funktion vertritt es Österreich unter anderem bei folgenden Institutionen:

- Europäische Agentur für Netz- und Informationssicherheit (ENISA) und
- Europäisches Forum für den Informationsaustausch zwischen den EU-Mitgliedstaaten in Bezug auf die Sicherheit und Robustheit von kritischer Informations-Infrastruktur (KII).

Die Mitgliedschaft bei der „European Government CERTs (EGC) group“ ist beantragt.

Über CERT.at ist Österreich weiters vertreten

- beim Forum for Incident Response and Security Teams (FIRST) und
- bei Trusted Introducer (TI).

Teilnahme am GovCERT

Teilnahmeberechtigt sind VertreterInnen von IKT-NutzerInnen aus dem Behördenbereich, das heißt Betreiber von „.gv.at“-Domains, zum Beispiel:

- Bundesministerien,
- Landesverwaltungen,
- Städte- und Gemeindeverwaltungen

sowie von Einrichtungen aus dem Bereich der kritischen Infrastruktur (KRITIS). Eine Liste der konkreten betroffenen Sektoren wird derzeit für den Masterplan „Österreichisches Programm zum Schutz kritischer Infrastruktur“ erarbeitet.

GovCERT-Verantwortliche müssen dem Bundeskanzleramt durch die jeweilige Behörde beziehungsweise den Infrastrukturbetreiber offiziell nominiert werden.

CERT.at

ist das österreichische nationale CERT (Computer Emergency Response Team), eine Initiative von nic.at, der österreichischen Domain-Registry, und wird von nic.at auch gesponsert.

Zielgruppe sind österreichische IT-Security-Teams und lokale CERTs. Als solches ist CERT.at der Ansprechpartner für IT-Sicherheit im nationalen Umfeld. Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur (KRITIS), IKT (Informations- und Kommunikationstechnik) und gibt Warnungen, Alerts und Tipps für KMUs (kleine und mittlere Unternehmen) heraus.

Bei Angriffen auf Rechner auf nationaler Ebene koordiniert CERT.at und informiert die jeweiligen Netzbetreiber und die zuständigen lokalen Security-Teams (siehe auch cert.at; Leitbild).

Weiters werden proaktiv Warnungen und Know-how an KMUs (kleine und mittlere Unternehmen) und die breite Öffentlichkeit weitergegeben, um so insgesamt ein sichereres Internet in Österreich zu schaffen.

Im Rahmen einer Kooperation mit dem Government Computer Emergency Response Team für die öffentliche Verwaltung (GovCERT) und die kritische Informations-Infrastruktur (KII) in Österreich stellt CERT.at seine Ressourcen für die Behandlung sicherheitsrelevanter Vorfälle in diesem Bereich zur Verfügung.

Es hat keine Weisungsgewalt über den österreichischen IP-Adressraum, es gibt jedoch starke Kontakte zu allen großen Internet Service Providern (ISPs) und dem ACOnet-CERT, dem CERT des österreichischen Forschungsnetzes ACOnet.

Siehe dazu:

- govCert.at
- cert.at
- ACOnet-CERT

16.2 Sicherheit von Netz- und Informationssystemen (NIS)

Mit dem Ziel EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme zu erreichen, wurde 2016 die Richtlinie (EU) 2016/1148 über „Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-RL) verabschiedet. Zur Anwendung der NIS-RL wurde 2018 die Durchführungsverordnung (EU) 2018/151 der Kommission über „Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls“ erlassen. In Österreich wurde die NIS-Richtlinie im Jahr 2018 mit dem Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt. Zusätzlich wurde die Netz- und Informationssystemsicherheitsverordnung (NISV) erlassen, welche Sektor-spezifische Sicherheitsvorkehrungen, wesentliche Dienste und die jeweiligen Arten von Sicherheitsvorfällen definiert, sowie die Verordnung über qualifizierte Stellen (QuaSteV) in der Anforderungen und das Prüfverfahren zur Feststellung qualifizierter Stellen enthalten sind.

Definition von Netz- und Informationssystemen

Ein Netz- und Informationssystem im Sinne des NIS-Gesetzes ist/sind:

- ein elektronisches Kommunikationsnetz im Sinne des § 3 Z 11 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003,
- räumlich verteilte, digitale Verarbeitungsvorrichtungen zur technischen Unterstützung der Erhebung, Verarbeitung, Speicherung, Wartung, Nutzung, Weitergabe, Verbreitung oder Disposition von digitalen Informationen,
- digitale Daten, die in einem solchen elektronischen Kommunikationsnetz oder in solchen Vorrichtungen verarbeitet werden.

Zweck und Umsetzung

Aus all diesen Regelwerken ergeben sich diverse Verpflichtungen für den Betrieb essenzieller Netz- und Informationssysteme, sofern diese in den Anwendungsbereich des NIS-Gesetzes fallen. Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind. Netz- und Informationssystemsicherheit trägt dazu bei, Gefährdungen zu erkennen, zu bewerten und zu verfolgen, die Fähigkeit zu stärken, Störungen zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wiederherzustellen.

In der NIS-Richtlinie ist unter anderem auch festgehalten, dass Mitgliedstaaten eine nationale NIS-Strategie erarbeiten müssen, die strategische Ziele, Prioritäten und Maßnahmen enthalten soll. Diese nationale NIS-Strategie wurde hierzulande durch die „Österreichische Strategie für Cyber Sicherheit“ umgesetzt. Die EU-weite Etablierung von nationalen zentralen Anlaufstellen vereinfacht die Zusammenarbeit zwischen den Mitgliedsstaaten im Falle von grenzüberschreitenden Störfällen. Weiters wird durch die jeweiligen nationalen NIS-Strategien und Meldeeinrichtungen auch das Sicherheitsniveau kritischer Dienste bzw. Infrastruktur in den Mitgliedsstaaten an sich gesteigert. Somit können Sicherheitsvorfälle schneller erkannt und abgewehrt werden und zukünftigen Vorfällen besser vorgebeugt werden.

Definition von Sicherheitsvorfällen

Ein Sicherheitsvorfall liegt vor, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes von erheblicher Auswirkung geführt hat. Der Dienst ist ein wesentlicher Dienst, ein digitaler Dienst oder ein wichtiger Dienst, den eine Einrichtung des Bundes erbringt.

Ein Sicherheitsvorfall kann neben Cyberangriffen oder Einwirkungen Dritter auch durch physische Ereignisse wie etwa Naturereignisse, aber auch durch Ereignisse wie z. B. Stromausfälle oder das Verhalten eigener Mitarbeiter verursacht werden.

Bei der Beurteilung, ob eine Störung erhebliche Auswirkungen hat und somit einen Sicherheitsvorfall darstellt, sind insbesondere die Anzahl der betroffenen Nutzer, die Dauer der Störung, die geografische Ausbreitung der Störung sowie die Auswirkung auf wirtschaftliche oder gesellschaftliche Tätigkeiten zu berücksichtigen.

Für die Betreiber wesentlicher Dienste sind die Parameter für die Beurteilung einer erheblichen Auswirkung in der NIS-Verordnung festgelegt. Im Falle von Anbietern digitaler Dienste sind die Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls in der Durchführungsverordnung (EU) 2018/151 festgelegt. Bei Einrichtungen der öffentlichen Verwaltung liegt die Beurteilung einer erheblichen Auswirkung im Ermessen der betroffenen Organisation.

Qualifizierte Stellen

Eine qualifizierte Stelle ist ein Unternehmen mit Hauptniederlassung oder Sitz in Österreich, das legitimiert ist, die Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste zu überprüfen. Die Voraussetzungen und das Verfahren für die Feststellung qualifizierter Stellen werden durch die Verordnung über qualifizierte Stellen (QuaSteV) festgelegt. Der Aufgabenbereich einer qualifizierten Stelle zeigt, welchen spezifischen Bereich der Sicherheitsvorkehrungen von dieser geprüft werden kann. Dieser kann von einzelnen Sicherheitsmaßnahmen bis hin zu mehreren bzw. allen Kategorien reichen. Die Sicherheitsvorkehrungen mit ihren Kategorien und einzelnen Sicherheitsmaßnahmen sind in der NIS-Verordnung festgelegt. Mit dem NIS Fact Sheet 7/2019 – Qualifizierte Stellen wurde ein Leitfaden für Antragstellerinnen und qualifizierte Stellen veröffentlicht, der unter Anderem den Ablauf des Verfahrens zur Feststellung von qualifizierten Stellen oder die Beurteilung von Prüfern näher ausführt.

Anlaufstellen in Österreich

Das Bundeskanzleramt betreibt in diesem Zusammenhang die Anlaufstelle Netz- und Informationssystemsicherheitsgesetz (NISG) unter https://www.nis.gv.at/, sowie das Büro für Strategische Netz- und Informationssystemsicherheit (NIS-Büro):

- Strategische NIS Behörde
  Bundeskanzleramt
  Abteilung I/8 – NIS Büro
  E-Mail: nis@bka.gv.at

Weiters wird im Innenministerium die zentrale Anlaufstelle (Single Point of Contact - SPOC) zur grenzüberschreitenden Zusammenarbeit betrieben:

- Operative NIS-Behörde
  Bundesministerium für Inneres
  E-Mail: nis@bvt.gv.at

16.2.1 Anwendungsbereich

Das NIS-Gesetz betrifft Betreiber wesentlicher Dienste in den Sektoren

- *Energie (Elektrizität, Erdöl, Erdgas),*
- *Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr),*
- *Bankwesen (Kreditinstitute),*
- *Finanzmarktinfrastrukturen (Handelsplätze, zentrale Gegenparteien),*
- *Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken),*
- *Trinkwasserversorgung (Unternehmen zur Lieferung von und Versorgung mit "Wasser für den menschlichen Gebrauch") und*
- *Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Registries)*

sowie – ab einer gewissen Größe – Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen oder Cloud-Computing-Dienste) und Einrichtungen der öffentlichen Verwaltung.

Betreiber wesentlicher Dienste werden durch einen Bescheid ermittelt. Die sich daraus ergebenden Verpflichtungen gelten daher auch erst ab Ausstellung des Bescheids. Um als solcher in Frage zu kommen und somit in den Anwendungsbereich des NIS-Gesetzes zu fallen, müssen neben der Tätigkeit in mindestens einem der genannten Sektoren zusätzlich noch gewisse Schwellenwerte erreicht sein. Diese sind in der NIS-Verordnung im zweiten Abschnitt definiert, worin für jeden der genannten Sektoren, weiter aufgeschlüsselt in Teilsektoren und Bereiche, konkrete zu erreichende Schwellenwerte beziehungsweise zu erfüllende Kriterien definiert sind. Ein Elektrizitätsunternehmen im Bereich der Stromerzeugung muss beispielsweise eine Erzeugungsanlage betreiben, die mehr als 340 MW Engpassleistung hat. Falls dieser Schwellenwert von 340 MW erreicht wird, entspricht das Unternehmen einem Betreiber wesentlicher Dienste und wird mittels Bescheid darüber in Kenntnis gesetzt. Ein aktives Ansuchen um einen Bescheid durch das Unternehmen ist nicht erforderlich.

Anbieter digitaler Dienste sind juristische Personen oder eingetragene Personengesellschaften, die zumindest einen der digitalen Dienste Online-Marktplatz, Online-Suchmaschine oder Cloud-Computing-Dienst anbieten und eine Hauptniederlassung in Österreich haben oder keine Hauptniederlassung in der Europäischen Union, aber einen Vertreter namhaft gemacht haben. Weiters sind Klein- und Kleinstunternehmen mit sowohl weniger als 50 Mitarbeitern als auch einem Jahresumsatz bzw. einer Jahresbilanz von weniger als 10 Millionen Euro ausgenommen. Sie werden im Gegensatz zu Betreibern wesentlicher Dienste nicht per Bescheid ermittelt, sondern müssen sich nach dem NIS-Gesetz selbst identifizieren.

Indirekt können auch weitere Unternehmen betroffen sein, sofern sie mit einem in den Anwendungsbereich fallenden Unternehmen Vertragsbeziehungen unterhalten. Hierbei sind jedoch nur vertragliche Verpflichtungen relevant und nicht solche, die durch das Gesetz direkt definiert wurden. Dieser Umstand rührt daher, dass ein in den Anwendungsbereich des NIS-Gesetzes fallendes Unternehmen gewisse Sicherheitsvorkehrungen treffen und auch nachweisen muss. Dabei ist die gesamte Kette an beteiligten Dienstleistern relevant. Ein Subunternehmen bzw. externer Dienstleister muss also zwangsweise zur Einhaltung gewisser Maßnahmen verpflichtet werden.

16.2.2 Verpflichtungen

Betroffene die in den Anwendungsbereich des NIS-Gesetzes fallen, müssen diverse Verpflichtungen erfüllen. Die Art und der Umfang dieser Verpflichtungen richten sich nach der jeweiligen Kategorie, also ob Betreiber wesentlicher Dienste, Anbieter digitaler Dienste oder Einrichtung der öffentlichen Verwaltung. Unabhängig von der Kategorie ist jedoch, dass grundsätzlich Vorkehrungen zum Schutz der IT-Systeme und Dienste getroffen werden müssen und dass eingetretene Sicherheitsvorfälle gemeldet werden müssen.

Betreiber wesentlicher Dienste müssen

- innerhalb von zwei Wochen nach Zustellung des Bescheides, mit dem sie als ein Betreiber wesentlicher Dienste gemäß § 16 Abs. 1 NISG ermittelt werden, eine Kontaktstelle (Single Point of Contact - SPOC) bekanntgeben (§ 16 Abs. 3 NISG). Hierzu müssen zumindest eine E-Mail-Adresse und Telefonnummer angegeben werden. Diese müssen auch nicht unbedingt einer konkreten Person zugeordnet sein – es wäre also auch eine office@...-Adresse zulässig. Voraussetzung ist jedoch, dass die Kontaktstelle in der Zeit erreichbar ist, in der man den wesentlichen Dienst anbietet. In der Regel werden diese Dienste jedoch ohnehin Rund um die Uhr bereitgestellt. Im NIS Fact Sheet 1/2019 – Kontaktstellen von Betreibern wesentlicher Dienste sind dazu ausführliche Erläuterungen verfügbar.
- angemessene technische und organisatorische Schutzmaßnahmen für ihre IT-Systeme umsetzen und dokumentieren, um Sicherheitsvorfällen vorzubeugen. Dies beinhaltet auch die Umsetzung geeigneter Maßnahmen für die zeitnahe Erkennung und korrekte Handhabung auftretender Sicherheitsvorfälle. Konkrete Sicherheitsmaßnahmen sind in Anlage 1 der NISV angeführt. Nähere Erläuterungen und Hilfestellungen zur Umsetzung zu den in Anlage 1 der NIS-Verordnung definierten Sicherheitsmaßnahmen finden sich im NIS Fact Sheet 8/2019 – Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste.

- mindestens alle drei Jahre einen Nachweis über ausreichende Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme erbringen. Dieser Nachweis kann durch Zertifizierungen erfolgen oder mittels Überprüfung durch eine qualifizierte Stelle. Dabei werden neben einer Aufstellung der vorhandenen Sicherheitsvorkehrungen auch die aufgedeckten Sicherheitsmängel übermittelt. Innerhalb eines Jahres nach Zustellung des Bescheids kann ein derartiger Nachweis jederzeit verlangt werden.
- im Falle eines Sicherheitsvorfalls unverzüglich eine Meldung an das zuständige nationale oder sektorenspezifische Notfallteam (z.B. CERT.at, GovCERT Austria, Austrian Energy CERT) weiterleiten.

Anbieter digitaler Dienste müssen

- geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen für die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, treffen. Sie sind aber grundsätzlich in deren Auswahl frei, sofern diese ein angemessenes Sicherheitsniveau gewährleisten und die Vorgaben der NIS-RL einhalten. Diese Sicherheitsvorkehrungen haben unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden mit vernünftigem Aufwand feststellbaren Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:
  - Sicherheit der Systeme und Anlagen,
  - Bewältigung von Sicherheitsvorfällen,
  - Betriebskontinuitätsmanagement,
  - Überwachung, Überprüfung und Erprobung,
  - Einhaltung der internationalen Normen.
- einen Sicherheitsvorfall, der einen digitalen Dienst betrifft, unverzüglich melden. Zuständig für die Entgegennahme der Meldung ist das nationale Computer-Notfallteam. Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. Die Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls sind in der Durchführungsverordnung (EU) 2018/151 festgelegt.
  Diese Meldung ist unabhängig von anderen Meldepflichten – beispielsweise aus der DSGVO – und ersetzt diese nicht. Sie muss weiters auch wirklich unverzüglich durchgeführt werden. So ist es in diesem Fall auch möglich bzw. sogar erwünscht eine unvollständige jedoch unverzügliche Meldung zu machen und weitere Details nachzuliefern, da gerade am Anfang eventuell noch gar nicht das gesamte Ausmaß ersichtlich ist.

Einrichtungen der öffentlichen Verwaltung müssen

- für die Netz- und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen treffen. Ein wichtiger Dienst der öffentlichen Verwaltung gemäß NIS-Gesetz ist entweder eine Sachgebietsverantwortung der Einrichtung, die von Netz- und Informationssystemen abhängig ist und bei der ein Sicherheitsvorfall diesen Dienst betreffend erhebliche Auswirkungen hat oder ein IKT-Dienst, dessen Ausfall oder Mangelfunktion zu einer erheblichen Beeinträchtigung der Funktionstüchtigkeit der Einrichtung führt. Im NIS Fact Sheet 9/2019 – Umsetzungsleitfaden für Einrichtungen des Bundes werden Einrichtungen der öffentlichen Verwaltung mit Kriterien für die Einstufung von wichtigen Diensten sowie Parametern zur Beurteilung der Erheblichkeit von Auswirkungen unterstützt.
- einen Sicherheitsvorfall, der einen wichtigen Dienst betrifft, unverzüglich melden (Pflichtmeldung). Zuständig für Einrichtungen der öffentlichen Verwaltung ist das Computer-Notfallteam der Öffentlichen Verwaltung „GovCERT“. Risiken und Vorfälle können auf freiwilliger Basis gemeldet werden (freiwillige Meldung).

Meldestellen

Verpflichtende Meldungen können – je nach Art des Dienstes bzw. der Einrichtung – bei einer der folgenden Meldestellen abgegeben werden. Darüber hinaus können Risiken und Vorfälle, die nicht unter die Meldeverpflichtung fallen, auch freiwillig gemeldet werden. Der Meldeweg unterscheidet sich grundsätzlich nicht von jenem für eine verpflichtende Meldung, jedoch können freiwillige Meldungen auch zeitverzögert, aggregiert und ohne namentliche Nennung der Melder gesendet werden.

- Meldeportal für öffentliche Verwaltungen (GovCERT Austria)
- Meldeportal für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste (CERT.at)
- Meldeportal für Betreiber wesentlicher Dienste im Sektor Energie (Austrian Energy CERT)

Sanktionen

Bei Verstoß gegen diese Verpflichtungen drohen Verwaltungsstrafen mit einem Strafrahmen bis zu 50.000 Euro, beziehungsweise im Wiederholungsfall bis zu 100.000 Euro.

17 Disaster Recovery und Business Continuity

17.1 Informationssicherheits-Aspekte des betrieblichen Kontinuitätsmanagements

17.1.1 Definition von Verfügbarkeitsklassen

Um den Verfügbarkeitsanspruch von IT-Anwendungen einer Organisation darstellen zu können, sind im Rahmen der IT-Sicherheitspolitik entsprechende Verfügbarkeitsklassen zu definieren (vgl. dazu auch 8.2.4 Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity-Planung).

Nachfolgend ein Beispiel für ein solches Klassifizierungsschema – basierend auf den Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich des Bundeskanzleramtes (Beschuss in der 11. IKT-Board-Sitzung vom 05.11.2002):

- **Betriebsverfügbarkeitskategorie 1 – Keine Vorsorge (unkritisch):**
  Für die IT-Anwendung werden keine besonderen Vorkehrungen getroffen. Es ist ein Datenverlust bzw. Ausfall der IT-Anwendung unbestimmter Dauer denkbar. Eine Behinderung in der Wahrnehmung der Aufgaben der betroffenen Verwaltungsstelle entsteht durch den Ausfall bzw. Datenverlust nicht.
- **Betriebsverfügbarkeitskategorie 2 – Offline Sicherung:**
  Es sind die gängigen Sicherungsmaßnahmen für die IT-Anwendung vorgesehen, ein Datenverlust ist auszuschließen. Die IT-Anwendung kann bei technischen Problemen erst nach deren Behebung am ursprünglichen Produktivsystem in Betrieb genommen werden. Die Sicherung wird an einen externen Ort ausgelagert.
- **Betriebsverfügbarkeitskategorie 3 – Redundante Infrastruktur:**
  Die Infrastruktur für die IT-Anwendung ist derart ausgelegt, dass bei Ausfall einer IT-Komponente der Betrieb durch redundante Auslegung ohne Unterbrechung fortgesetzt werden kann.
- **Betriebsverfügbarkeitskategorie 4 – Redundante Standorte:**
  Die IT-Infrastruktur sowie die darauf aufsetzende IT-Anwendung ist auf zwei Standorte verteilt, so dass bei Betriebsunterbrechung des einen Standortes die IT-Anwendung uneingeschränkt am zweiten Standort weiter betrieben werden kann.

Zusätzlich zu den vier genannten Kategorien ist noch die Zusatzqualität „K-Fall sicher“ definiert, welche auch die Anforderungen in Katastrophenfällen berücksichtigt:

- **K-Fall sicher (K2 bis K4):**
  Die IT-Anwendung ist derart konzipiert, dass zumindest ein Notbetrieb in einer Zero-Risk-Umgebung möglich ist. Dazu werden die Daten je nach Aktualisierungsgrad laufend in die Zero-Risk-Umgebung transferiert und der Betrieb der IT-Anwendung derart gestaltet, dass ein Wiederaufsetzen eines definierten Notbetriebes in der Zero-Risk-Umgebung umgehend möglich ist. Eine Einbindung der Zero-Risk-Umgebung in den Normalbetrieb ist je nach Sensibilität vorgesehen.

In Summe ergibt eine derartige Einstufung die Verfügbarkeitsklassen 1 bis 4 und K2 bis K4. Die Zusatzoption „K-Fall sicher“ in Verbindung mit Betriebsverfügbarkeitskategorie 1 ist nicht sinnvoll.

17.1.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

Für die in einem IT-System betriebenen IT-Anwendungen und deren Daten sind die Verfügbarkeitsanforderungen festzustellen. Da eine IT-Anwendung nicht zwingend jeden Bestandteil des IT-Systems benötigt, sind die Verfügbarkeitsanforderungen der IT-Anwendungen auf die wesentlichen Komponenten des IT-Systems abzubilden.

Das Ergebnis dieser Arbeit kann in Form einer Übersicht dargestellt werden, wie das nachfolgende Beispiel illustrieren soll:

IT-Anwendung	Verfügbarkeitsklasse (lt. Beispiel in 17.1.1)	IT-System	IT-Komponente
Prozessleitsystem	Kategorie 3, K-Fall sicher (K3)	Prozessleitrechner	Host-Prozessleitsystem
			Datenhaltung
		Netzwerk	Leitungen
			Switching-/Routing-Devices
Buchhaltung	Kategorie 2	Zugangssystem	Host-Zugangssystem
		Rechensystem	Datenhaltung
		Netzwerk	Leitungen
			Switching-/Routing-Devices

Tabelle 17.1: Verfügbarkeitsklassen der Anwendung

Die zu fordernde Betriebsverfügbarkeit der Systeme und Komponenten wird durch deren Anwendung definiert. Demnach wurde in obiger Tabelle vordergründig die Verfügbarkeit der einzelnen Anwendungen aufgeführt und in weiterer Folge alle zur Ausführung der Anwendung notwendigen Komponenten und Systeme aufgelistet. Über die Identifikation der Komponenten lassen sich gemeinsam genutzte Systemteile identifizieren und deren Verfügbarkeitskategorie festlegen. Die Anwendung mit höchster Kategorie ist dabei bestimmend, wie in folgender Tabelle dargestellt:

IT-System	IT-Komponente	Verfügbarkeitsklasse (lt. Beispiel in 17.1.1)	Bestimmende Anwendung
Zugangssystem	Host-Zugangssystem	Kategorie 2	Buchhaltung
Rechensystem	Datenhaltung	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
Prozessleitrechner	Host-Prozessleitsystem	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	Datenhaltung	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
Netzwerk	Leitungen	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem
	Switching-/Routing-Devices	Kategorie 3, K-Fall sicher (K3)	Prozessleitsystem

Tabelle 17.2: Verfügbarkeitsklassen der Systeme und Komponenten

Dies ist wie folgt zu interpretieren: Die IT-Komponente „Host-Zugangssystem“ im IT-System „Zugangssystem“ hat aufgrund der IT-Anwendung „Buchhaltung“ eine maximal tolerierbare Ausfallzeit von 3 Stunden und ist daher der Verfügbarkeitsklasse 2 zuzuordnen.

Eine praktikable Vorgehensweise ist es, zu den einzelnen IT-Anwendungen den zuständigen Applikationsverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse nach IT-System und Komponenten geordnet in der Tabelle aufzuführen. Die Anforderungen an die Verfügbarkeit sind zu begründen, sofern dies nicht schon an anderer Stelle geschehen ist. Die Verfügbarkeitsanforderungen sind von der Behörden- bzw. Unternehmensleitung zu bestätigen.

Die Tabelle ist regelmäßig zu überprüfen und gegebenenfalls zu aktualisieren.

Die Übersicht erleichtert es, die besonders zeitkritischen Komponenten des IT-Systems zu extrahieren, für die die Notfallvorsorge unumgänglich ist. Bei Ausfall einer Komponente gibt diese Übersicht Auskunft über die betroffenen IT-Anwendungen und deren Verfügbarkeitsanforderungen.

Bei Ausfall einer Komponente des IT-Systems ermöglicht diese Übersicht weiters eine schnelle Aussage, ab wann ein Notfall vorliegt. Nicht jeder Teil- oder Gesamtausfall des Systems stellt einen Notfall dar. Oftmals lassen sich Ausfälle des IT-Systems durch geplante Maßnahmen, z. B. Ersatzbeschaffung, auch in kurzer Zeit beheben. Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt.

Dass ein Notfall auch bei Ausfall einer besonders zeitkritischen Komponente nicht zwingend eintreten muss, lässt sich anhand des Ersatzbeschaffungsplans (siehe 17.1.10 Ersatzbeschaffungsplan) und der Untersuchung über interne und externe Ausweichmöglichkeiten (vgl. 17.1.7 Untersuchung interner und externer Ausweichmöglichkeiten) ersehen.

17.1.3 Benennung einer/eines Notfallverantwortlichen

Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen.

Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung einer/eines Notfallverantwortlichen. Die Behörden- bzw. Unternehmensleitung muss die Notfallverantwortliche/den Notfallverantwortlichen sowohl für die Entscheidung, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen, autorisieren.

17.1.4 Erstellung eines Disaster Recovery-Handbuches

In einem Disaster Recovery-Handbuch (auch als Notfallhandbuch bezeichnet) sind alle Maßnahmen, die nach Eintritt eines notfallauslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen zu dokumentieren. Das Disaster Recovery-Handbuch ist so zu gestalten, dass sachverständige Dritte in der Lage sind, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

In Anhang B.13 wird beispielhaft ein umfassendes Inhaltsverzeichnis eines Disaster Recovery-Handbuches zur Orientierung aufgeführt. Welche Teile dieses Vorschlags übernommen werden können, ist abhängig von der vorhandenen System- und Anwendungsdokumentation und kann daher nur individuell entschieden werden.

Das Disaster Recovery-Handbuch ist durch die Leitung der Organisation in Kraft zu setzen und muss nach Bedarf aktualisiert werden. Die Verfügbarkeit des Disaster Recovery-Handbuchs ist von zentraler Bedeutung. Deshalb ist ein aktuelles Exemplar extern (als „Hardcopy“) auszulagern. Zusätzlich ist das Disaster Recovery-Handbuch allen im Handbuch genannten Personen oder Organisationseinheiten zur Kenntnis zu bringen.

17.1.5 Definition des eingeschränkten IT-Betriebs (Notlaufplan)

Für den Fall, dass Teile des IT-Systems ausfallen, ist zu untersuchen, ob ein eingeschränkter IT-Betrieb notwendig und möglich ist. Um bei einem eingeschränkten IT-Betrieb möglichst viele IT-Anwendungen betreiben zu können, ist die für jede einzelne IT-Anwendung zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren.

Für den eingeschränkten IT-Betrieb muss festgelegt werden, welche IT-Anwendungen mit welcher Priorität betrieben werden. Dies ist schriftlich zu fixieren (Notlaufplan).

Auch manuelle Ersatzverfahren können geeignet sein, um die Verfügbarkeitsanforderungen einer IT-Anwendung zu senken. Die für den Einsatz eines manuellen Ersatzverfahrens erforderlichen Hilfsmittel (Formulare, Papierlisten, Mikrofiche) müssen dazu allerdings bereitgehalten werden.

Die qualitativen und quantitativen Vorgaben für den eingeschränkten IT-Betrieb sind mit den Fachbereichen abzusprechen.

17.1.6 Regelung der Verantwortung im Notfall

Für den Zeitraum von Eintritt des schädigenden Ereignisses bis zur vollständigen Wiederherstellung der Verfügbarkeit kann eine zeitlich befristete Notfallorganisation erforderlich sein.

Es müssen Verantwortliche bestimmt sein, die befugt sind zu entscheiden, ob ein Notfall eingetreten ist, und die die entsprechenden Maßnahmen des Disaster Recovery-Handbuchs einleiten (siehe 17.1.3 Benennung einer/eines Notfallverantwortlichen). Die an der Durchführung der Maßnahmen im Bereich der Notfallvorsorge beteiligten Organisationseinheiten müssen befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten. Dieses „Notfallorganigramm“ muss von der Leitung der Organisation autorisiert werden.

17.1.7 Untersuchung interner und externer Ausweichmöglichkeiten

Um Kapazitätsengpässe im eingeschränkten IT-Betrieb zu vermeiden, sind interne und externe Ausweichmöglichkeiten zu untersuchen.

Bei der Untersuchung von Ausweichmöglichkeiten ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung.

Zunächst steht die interne Verlagerung von IT-Anwendungen von einem IT-System auf ein anderes IT-System im Vordergrund (z. B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können. Dabei ist dafür Sorge zu tragen, dass die Integrität und Vertraulichkeit der ausgelagerten IT-Anwendungen und Daten gewährleistet wird.

Ebenso sind Ausweichmöglichkeiten für nicht IT-spezifische Komponenten zu berücksichtigen. So sind beispielsweise im Bereich der Infrastruktur Ausweichmöglichkeiten für IT-Räume in Betracht zu ziehen.

Auf Basis des IKT-Board-Beschlusses [IKTB-170902-4] sind für Organisationen der öffentlichen Verwaltung einheitliche Kriterien für Ausweichsysteme und für die Krisensicherung empfohlen. Dazu sind Kriterienkataloge anzuwenden, die mit den jeweiligen entsprechenden Ressorts abgestimmt worden sind. Die Ausweichstandorte werden in Bezug auf die Erfüllung der Klassen des Kriterienkataloges klassifiziert.

Die Konfiguration, Kapazität und Kompatibilität von internen und externen Ausweichmöglichkeiten sind dem aktuellen Verfahrensstand anzupassen.

17.1.8 Alarmierungsplan

Ein Alarmierungsplan enthält eine Beschreibung der Meldewege, über die bei Eintritt eines Notfalls die zuständigen Personen oder Organisationseinheiten zu informieren sind. Die Alarmierung kann z. B. über Telefon, Fax, Funkrufdienste oder Kurier erfolgen. Beschrieben werden muss, wer wen benachrichtigt, wer ersatzweise zu benachrichtigen ist bzw. wie bei Nichterreichen zu verfahren ist.

Zu diesem Zweck sind evtl. Adress- und Telefonlisten zu führen. Wird eine Evakuierung des Gebäudes nötig bzw. ist dieses nicht betretbar (Brand-, Bombenalarm, …), müssen entsprechende Treffpunkte vereinbart sein.

Der Alarmierungsplan muss sämtlichen Notfallverantwortlichen zur Verfügung stehen, darüber hinaus an zentraler Stelle redundant vorgehalten werden (z. B. Portier, Bewachungspersonal). Die im Alarmierungsplan genannten Personen müssen den sie betreffenden Teil kennen. Allen MitarbeiterInnen müssen die AnsprechpartnerInnen bekannt sein, denen das Eintreten eines evtl. notfallauslösenden Ereignisses gemeldet werden kann.

Es kann verschiedene Alarmierungspläne für unterschiedliche Schadensfälle (Feuer, Wasser, Strom- und Netzwerkausfall) geben. Dabei muss darauf geachtet werden, dass alle Schadensfälle abgedeckt sind.

Mit der Erstellung eines Alarmierungsplans sollte auch die Festlegung eines Ruf- oder Bereitschaftsdienstes erwogen werden.

Der Alarmierungsplan ist immer aktuell zu halten und regelmäßig zu testen.

17.1.9 Erstellung eines Wiederanlaufplans

Für einen geregelten Wiederanlauf nach Ausfall einer IT-Komponente sind folgende Informationen zu dokumentieren (siehe Beispiel in B.13 Inhaltsverzeichnis Disaster Recovery-Handbuch (Muster)):

- Wiederbeschaffungsmöglichkeiten, zum Beispiel die Nutzung eines Testrechners für den Echtbetrieb oder die Ersatzbeschaffung (siehe 17.1.10 Ersatzbeschaffungsplan),
- interne/externe Ausweichmöglichkeiten für IT-Anwendungen (siehe 17.1.7 Untersuchung interner und externer Ausweichmöglichkeiten) sind aufzuzählen,
- DFÜ-Versorgung (Datenfernübertragung) für den Notbetrieb, um die minimal notwendigen Datenübertragungen zu gewährleisten,
- die im eingeschränkten IT-Betrieb (siehe 17.1.5 Definition des eingeschränkten IT-Betriebs (Notlaufplan)) laufenden IT-Anwendungen sowie
- Systemstart der IT-Komponente und Einbindung in das IT-System.

Um den Anforderungen an die Verfügbarkeit (siehe 17.1.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen) der einzelnen IT-Anwendungen gerecht zu werden, ist eine Reihenfolge für den Wiederanlauf der IT-Anwendungen festzulegen.

Die für den Wiederanlauf einer IT-Anwendung erforderlichen Schritte sind im Disaster Recovery-Handbuch (siehe 17.1.4 Erstellung eines Disaster Recovery-Handbuches) aufzuzeigen. Beispiele für solche Schritte sind:

- Aufbau und Installation der notwendigen Hardwarekomponenten,
- Einspielen der Systemsoftware,
- Einspielen der Anwendungssoftware,
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien,
- Wiederanlauf.

Eine revisionsfähige Protokollierung des Wiederanlaufs ist zu gewährleisten.

Der Wiederanlaufplan ist durch Notfallübungen (sowohl bei internen als auch bei externen Ausweichmöglichkeiten) auf seine Durchführbarkeit zu testen. Insbesondere ist bei der Durchführung solcher Übungen der ausschließliche Einsatz der Software und Daten zu testen, die in internen oder externen Sicherungsarchiven aufbewahrt werden.

Der Wiederanlauf kann, je nach Umfang der betriebenen IT-Anwendungen, mit erheblichem Zeitaufwand verbunden sein. Der Zeitaufwand für die mit dem Wiederanlauf verbundenen Maßnahmen kann durch solche Übungen ermittelt werden und ist bei der Überarbeitung des Wiederanlaufplans zu berücksichtigen.

17.1.10 Ersatzbeschaffungsplan

Bei Ausfall einzelner Teile des IT-Systems ist neben der Reparatur die Ersatzbeschaffung zunächst die Maßnahme, die am zielgerichtetsten die Wiederherstellung der Verfügbarkeit verfolgt.

Um den Vorgang der Ersatzbeschaffung zu beschleunigen, ist die Erstellung eines Ersatzbeschaffungsplans sinnvoll. Dieser muss für jede wichtige IT-Komponente Angaben machen über:

- Bezeichnung der IT-Komponente (Name, Geräte-Nr., Beschaffungsdatum),
- Hersteller,
- Lieferant,
- Lieferzeit und
- Dauer der Reinstallation.

Ersatzbeschaffungsmaßnahmen müssen neben der Wiederherstellung der Verfügbarkeit des IT-Systems auch der Fortentwicklung der Informationstechnik Rechnung tragen. Entsprechen eingesetzte Teile des IT-Systems nicht mehr dem Stand der Technik, so darf eine Ersatzbeschaffung nicht ausschließlich darauf gerichtet sein, den alten Zustand wiederherzustellen. Dies erfordert eine regelmäßige Überarbeitung des Ersatzbeschaffungsplans. Der Bezug zur Betriebsmittelverwaltung ist zu beachten (vgl. 8.3.1 Betriebsmittelverwaltung).

17.1.11 Lieferantenvereinbarungen

Bei Kauf von Informationstechnik ergibt sich für die IT-BetreiberInnen die Notwendigkeit, Ersatzbeschaffungsmaßnahmen zu planen. Von besonderer Bedeutung beim Kauf sind eine vom Hersteller oder Lieferanten zugesicherte Nachkaufgarantie, Ersatzteillieferung, garantierte Lieferzeiten, die Garantiezeit bei auftretenden Mängeln sowie der angebotene Support.

Miet- bzw. Leasingverträge müssen Regelungen über schadensvorbeugende Wartungsarbeiten und die Anforderungen an die Beseitigung von Störungen oder Schäden beinhalten.

Im Gegensatz zum Kauf von Informationstechnik ist bei deren Miete oder Leasing eine Vielzahl von Risiken über den Vermieter bereits abgesichert. In der Regel schließen VermieterInnen eine Feuerversicherung für die vermietete Informationstechnik ab, die von der MieterInnen durch den Mietvertrag mitbezahlt wird. Somit ist bei Miete oder Leasing von Informationstechnik auf die nicht vom Vertrag abgedeckten Versicherungslücken zu achten.

17.1.12 Abschließen von Versicherungen

Das trotz aller informationstechnischen, baulichen und organisatorischen Maßnahmen verbleibende Restrisiko kann durch entsprechende Versicherungen abgedeckt werden.

Für Bundesbehörden ist der Abschluss von Versicherungen zwar unüblich, dennoch sollen die prinzipiellen Möglichkeiten im Folgenden angeführt werden.

Da die herkömmlichen Geschäftsversicherungen gegen Feuer, Diebstahl oder Sturm nur bestimmte Gefahren abdecken („Ausschnittsdeckung“), nicht aber die spezifischen Risiken im Bereich der Datenverarbeitung, kann der Abschluss eigener DV-Versicherungen notwendig werden.

Im Folgenden werden derzeit in Österreich angebotene Sparten von Computerversicherungen kurz erörtert. Da die Versicherungsbedingungen von den einzelnen Anbietern individuell festgelegt werden können, sind Details zu den einzelnen Sparten, ihrem Deckungsumfang und ihren Besonderheiten den konkreten Versicherungsbedingungen und -verträgen zu entnehmen. (Unverbindliche) Empfehlungen werden in den unten angeführten Musterbedingungen gegeben. Generell ist beim Abschluss von DV-Versicherungen aufgrund der Komplexität der Materie eine intensive Zusammenarbeit mit den Versicherungsgesellschaften anzustreben, um eine optimale Risikoabdeckung zu gewährleisten.

Elektronik-Sachversicherung

Dies ist die eigentliche Geräteversicherung. Ihr liegen als Musterbedingung die „Allgemeinen Bedingungen für die Versicherung von elektronischen Datenverarbeitungsanlagen“ (ADVB) zugrunde. Versicherte Gefahren und Schäden sind hier unvorhergesehen und plötzlich eintretende Beschädigung oder Zerstörung sowie der Verlust der versicherten Sachen etwa durch Bedienungsfehler, Fahrlässigkeit oder Sabotage (sofern die durch vorangeführte Gefahren verursachten Beschädigungen visuell ohne Hilfsmittel erkennbar sind), Wasser oder Feuchtigkeit, Brand, Blitzschlag, Explosionen, Diebstahl u. a. (Details siehe Artikel 2, §1 der ADVB).

Bei Abschluss der Versicherung ist insbesondere zu klären, welche Gegenstände versichert sind, und ob Voraussetzungen für bestimmte Leistungen bestehen, wie z. B. der Abschluss eines Wartungsvertrages.

Festzusetzen sind weiters die Versicherungssumme, die Angleichung der Versicherungssumme, der Versicherungsort, Selbstbehalte sowie mögliche Ausschlüsse und Erweiterungen. Es wird grundsätzlich der Neuwert (eventuell unter Abzug eines Selbstbehaltes) ersetzt.

Informationsverlust- und Datenträgerversicherung

Die Informationsverlust- und Datenträgerversicherung (vgl. auch „Allgemeine Bedingungen für die Informationsverlust- und Datenträgerversicherung elektronischer Datenverarbeitungsanlagen“ (ADVBID)) versichert die in der Polizze angeführten Datenträger und die auf ihnen befindlichen Daten unter den im Antrag angegebenen Betriebs- und Aufbewahrungsverhältnissen. Die Daten sind nur insoweit versichert, als sie wiederbeschaffbar und für die VersicherungsnehmerInnen erforderlich sind.

Ersetzt werden die Kosten für die Wiederherstellung von in Verlust geratenen Datenbeständen sowie der Wert zerstörter oder verlorener Datenträger.

Es ist jedoch zu beachten, dass diese Leistungen an eine Reihe von Bedingungen geknüpft sind.

Mehrkostenversicherung

Diese Versicherung deckt die Mehrkosten, die bei Störung bzw. Ausfall der DV-Anlage infolge eines durch die Sachversicherung gedeckten Schadensereignisses bei Weiterführung des Betriebes - etwa in einem Back-Up-Rechenzentrum - entstehen. Musterbedingungen sind die „Allgemeinen Bedingungen für die Mehrkostenversicherung elektronischer Datenverarbeitungsanlagen“ (ADVBM).

Betriebsunterbrechungsversicherung

Die Computerbetriebsunterbrechungsversicherung deckt den Ertragsausfall ab, den ein Unternehmen infolge eines ersatzpflichtigen Sachschadens erleidet.

Es gibt jedoch eine Reihe von Einschränkungen für die Ersatzleistung. Besondere Beachtung ist der Abgrenzung zur Feuerbetriebsunterbrechungsversicherung zu schenken.

Computermissbrauchversicherung

Die Computermissbrauchversicherung bietet Schutz gegen Schäden infolge von Computerkriminalität.

17.1.13 Redundante Leitungsführung

Bei der redundanten Leitungsführung werden zwischen geeigneten Punkten im Netz neben den im normalen Betrieb genutzten Leitungen zusätzliche Verbindungen eingerichtet.

Diese sollten über eine andere Trasse und wenn möglich von anderen Netzwerkknoten geführt werden. Dadurch besteht die Möglichkeit, bei Störungen auf die redundante Verbindung umzuschalten. Diese Umschaltung kann automatisch oder von Hand erfolgen. Die automatische Umschaltung ist an einer Stelle anzuzeigen, die die Störungsbeseitigung auf der normalen Leitung veranlasst.

Die Funktionsfähigkeit von redundanten Leitungen ist in sinnvollen Zeitabständen durch tatsächliche Nutzung auf ihre Funktionsfähigkeit hin zu überprüfen. Die Dimensionierung, die Prüfintervalle und die grundsätzliche Notwendigkeit von redundanten Leitungen sind direkt von den Verfügbarkeitsanforderungen an das Netz abhängig. Ebenso muss man das Verhältnis der Bereitstellungszeit der redundanten Leitung zur Wiederherstellungszeit der normalen Leitung berücksichtigen. Es ist allerdings von entscheidender Bedeutung, ob es sich um Leitungen im öffentlichen oder im privaten Bereich handelt.

Bei Leitungen im öffentlichen Bereich haben die BenutzerInnen keinen Einfluss auf deren Schutz. Das öffentliche Netz stellt grundsätzlich eine ausreichende Zahl von redundanten Leitungen zur Verfügung. Meistens reicht es aus, bei Ausfall einer Verbindung (gleichgültig ob Festverbindung oder Wählleitung) durch Aufbau einer Wählleitung die Verbindung wiederherzustellen. Die Schaltung von redundanten Festverbindungen ist in der Regel zu teuer und - wenn es nicht besondere Anforderungen z. B. betreffend Bandbreite gibt - meistens verzichtbar.

In einem privaten Netz können die BetreiberInnen die Sicherheit von Leitungen wesentlich beeinflussen. Kostenüberlegungen führen meist dazu, dass es keine redundanten Leitungen gibt. In privaten Netzen verursachen redundante Leitungen jedoch außer den Herstellungskosten keine laufenden Ausgaben.

Neben der redundanten Auslegung der Kommunikationsverbindungen ist auch zu überlegen, ob - auch bei Vorhandensein einer zentralen Notstromversorgung - die Notwendigkeit einer redundanten Stromanbindung besteht.

17.1.14 Redundante Auslegung der Netzkomponenten

An die Verfügbarkeit der zentralen Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele BenutzerInnen vom reibungslosen Funktionieren eines lokalen Netzes abhängig sind. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, ist in Abhängigkeit der entsprechenden Verfügbarkeitsanforderungen im jeweiligen Bereich Redundanz zu schaffen, die einem Teil- oder Totalausfall der relevanten Netzkomponenten mit akzeptablem Aufwand vorbeugt.

Dabei gibt es drei verschiedene Möglichkeiten, Redundanz zu erreichen:

1. Die Netzkomponenten können redundant im Lager vorgehalten werden, um in einem Notfall kurzfristig einen Austausch durchführen zu können. Wird dies nicht beachtet, sind oft langwierige Beschaffungsvorgänge nötig, bevor die Störung behoben werden kann.
2. Alternativ sind Wartungs- bzw. Lieferverträge mit den entsprechenden Herstellern abzuschließen, die einen schnellen Ersatz defekter Komponenten garantieren (siehe auch 17.1.10 Ersatzbeschaffungsplan). Danach können die gesicherten Konfigurationsdaten wieder eingespielt werden, um die Ausfallzeit der betroffenen Netzsegmente so gering wie möglich zu halten.

3. Es ist weiters sinnvoll, bereits bei der Konzeption des Netzes eine redundante Auslegung der Netzkomponenten einzuplanen. So sollten alle zentralen Switches und je nach den verwendeten Protokollen alle Router zumindest doppelt in das Netz eingebunden sein, um die Anbindung der Server und die Verbindung zwischen den einzelnen Netzkomponenten redundant zu halten. Die korrekte Funktionsweise ist durch eine geeignete logische Netzkonfiguration zu gewährleisten.

Ist je nach Verfügbarkeitsanforderungen auch eine Redundanz im Endgeräte-Bereich nötig, so müssen zusätzlich alle Endgeräte mit zwei Netzadaptern ausgerüstet werden.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind. Im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann ein geeignetes Redundanzkonzept entwickelt werden, welches diesen Anforderungen genügt. In diesem Zusammenhang ist auch 17.1.13 Redundante Leitungsführung zu beachten.

17.2 Umsetzung und Test

17.2.1 Durchführung von Disaster Recovery-Übungen

Disaster Recovery-Übungen dienen der Prüfung der Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge. Einerseits wird durch eine Notfallübung der effektive und reibungslose Ablauf eines Disaster Recovery-Planes erprobt und andererseits werden bisher unerkannte Mängel aufgedeckt.

Typische Übungen sind:

- die Durchführung einer Alarmierung,
- Durchführung von Brandschutzübungen,
- Funktionstests von Stromaggregaten,
- Wiederanlauf nach Ausfall einer ausgewählten IT-Komponente, wenn möglich unter Einbindung von (ausgewählten) IT-AnwenderInnen und
- Wiedereinspielen von Datensicherungen (vgl. 17.2.2 Übungen zur Datenrekonstruktion).

Die Ergebnisse einer Disaster Recovery-Übung sind zu dokumentieren.

Disaster Recovery-Übungen sind regelmäßig zu wiederholen. Da diese Übungen den normalen Betriebsablauf stören können, sollte die Häufigkeit an der Gefährdungslage orientiert sein, **jedoch sollten die entsprechenden Disaster Recovery-Übungen zumindest einmal jährlich stattfinden**. Soweit erforderlich sind Schulungsmaßnahmen der MitarbeiterInnen durchzuführen (Erste Hilfe, Brandbekämpfung etc.)

Vor Durchführung einer Disaster Recovery-Übung ist das Einverständnis der Leitung der Organisation einzuholen.

Aufgedeckte Mängel müssen Konsequenzen, wie etwa eine Überarbeitung der Disaster Recovery-Pläne, nach sich ziehen.

17.2.2 Übungen zur Datenrekonstruktion

> *Durch technische Defekte, falsche Parametrisierung, eine unzureichende Datenträgerverwaltung oder die Nichteinhaltung von Regeln, die in einem Datensicherungskonzept gefordert werden, ist es möglich, dass eine Rekonstruktion eines Datenbestandes nicht durchführbar ist. Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss daher sporadisch, zumindest aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Hierbei muss nachgewiesen werden, dass eine vollständige Datenrekonstruktion möglich ist.*

Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch VertreterInnen die Datenrekonstruktion vornehmen können, und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht (siehe 17.1.1 Definition von Verfügbarkeitsklassen und 17.1.2 Erstellung einer Übersicht über Verfügbarkeitsanforderungen).

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten ggf. auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

Es ist sicherzustellen, dass auch sachverständige Dritte die Datenrestaurierung anhand der vorhandenen Dokumentation durchführen können.

18 Security Compliance

18.1 Security Compliance Checking und Monitoring

> *Zur Gewährleistung eines angemessenen und gleich bleibenden Sicherheitsniveaus ist dafür Sorge zu tragen, dass alle Maßnahmen so eingesetzt werden, wie es im IT-Sicherheitskonzept und im IT-Sicherheitsplan vorgesehen ist. Dies muss für alle IT-Systeme, Projekte und Applikationen sichergestellt sein.*

Weiters sind die getroffenen Maßnahmen regelmäßig auf Übereinstimmung mit gesetzlichen und betrieblichen Vorgaben zu überprüfen.

Security Compliance Checks sollten zu folgenden Zeitpunkten bzw. bei Eintreten folgender Ereignisse durchgeführt werden:

- für neue IT-Systeme oder relevante neue Anwendungen:
  nach der Implementierung
- für bereits in Betrieb befindliche IT-Systeme oder Applikationen:
  nach einer bestimmten, in der IT-Systemsicherheitspolitik vorzugebenden Zeitspanne (z. B. jährlich) sowie bei signifikanten Änderungen.

18.1.1 Unabhängige Audits der Sicherheitsmaßnahmen

> *Das angestrebte Sicherheitsniveau wird in der Regel nicht auf einmal bzw. mit einer einzelnen Maßnahme erreicht, und bleibt nicht ohne Weiteres dauerhaft bestehen. Organisation, Infrastruktur und Umfeld sind immer wieder Änderungen unterworfen.*

Dies umfasst:

- neue Geschäftsprozesse
- neue Anwendungen
- neue Hard-, Software
- neue oder veränderte Infrastrukturen (Gebäude, Büros, Leitungen, Netzwerke)
- veränderte Organisationen (Outsourcing)
- neue MitarbeiterInnen in Schlüsselpositionen

oder:

- neue oder veränderte Gefährdungen (Nachbarfirmen mit Gefährdungspotenzialen)
- neue Angriffstechnologien

- veränderte Vermögenswerte und damit neuer Schutzbedarf
- Kenntnis von neuen Schwachstellen
- bereits eingetretene Sicherheitsvor- oder Schadensfälle

aber auch:

- Planungsänderungen, Terminverzug bei der Umsetzung von Sicherheitsmaßnahmen.

Prüfziel und Prüfzweck:

Dies erfordert die regelmäßige Überprüfung (Audit) aller Sicherheitsmaßnahmen. Sie sollte durch eine weitgehend unabhängige und kompetente Stelle (Revisionsabteilung oder spezialisierte externe Gutachter) erfolgen:

- damit nicht nur die unternehmenseigene Sichtweise zum Tragen kommt,
- die Ergebnisse nicht angezweifelt werden können und
- die Gelegenheit zum Einbringen zusätzlicher Expertise genutzt werden kann.

Keinesfalls sollten Personen als Prüfer tätig sein, die am Sicherheitskonzept mitgewirkt haben.

Geprüft werden die Maßnahmen laut Sicherheitskonzept:

- ob damit die angestrebten Sicherheitsziele erreicht werden können,
- ob sie zum Zeitpunkt der Prüfung noch umsetzbar, aktuell und vollständig sind,
- ob bzw. inwieweit sie umgesetzt (vorhanden, wirksam, dokumentiert) sind und auch gelebt werden.

Durchführung der Prüfungen:

Die laufenden Umsetzungsaktivitäten selbst sind hinsichtlich Umsetzungsstatus, Termintreue, Ressourceneinsatz und Kosten zu prüfen.

Solche Prüfungen sollten:

- vom Management initiiert und begleitet sein
- regelmäßig durchgeführt werden (zumindest einmal pro Jahr)
- aber auch zwischenzeitlich und unangekündigt erfolgen, insbesondere bei Änderungen in der Organisation.

Ziel der Prüfung ist nicht Überwachung der MitarbeiterInnen als Selbstzweck oder gar deren Bloßstellung, sondern:

- Suche nach und Eliminierung von Fehlerquellen, Schwachstellen und Mängeln
- Abgleich, ob
    - die Sicherheitsmaßnahmen gemäß Sicherheitskonzept umgesetzt sind oder werden

    - technische Maßnahmen korrekt implementiert bzw. konfiguriert sind
    - Auswertungen (etwa von Protokollen) tatsächlich durchgeführt werden und Auffälligkeiten beachtet werden
- Erkennen von
    - schwachen oder nicht wirksamen Sicherheitsmaßnahmen
    - nicht eingehaltenen Sicherheitsanweisungen und den Ursachen dafür
    - neuen oder veränderten Bedrohungen
- Anpassungsbedarf für das Sicherheitskonzept bzw. Sicherheitsmaßnahmen (Eignung, die Sicherheitsziele zu erreichen, ob nicht wirtschaftlichere Maßnahmen möglich sind)
- Schlußfolgerungen aus Sicherheitsvorfällen
- Verhindern, dass sich Sicherheitsvorfälle wiederholen
- Aufzeigen von Verbesserungs- und Korrekturmaßnahmen

Wesentlich für den Erfolg der Prüfung im Sinne eines Verbesserungspotenzials ist die Akzeptanz und Offenheit seitens aller Beteiligter. Daher muss ihnen der Nutzen dargestellt und allfällige Ängste vor Schuldzuweisungen genommen werden. Ansonsten würden womöglich bekannte Schwachstellen oder gar Vorfälle verschwiegen oder heruntergespielt.

Die Durchführung der Prüfung muss vom Management wie jedes andere Projekt koordiniert und begleitet werden. Immerhin bedeutet sie eine Zusatzbelastung für die MitarbeiterInnen, die zeitlich bzw. bisweilen auch räumlich ausreichend unterzubringen ist. Es sollte einerseits auf Effizienz geachtet werden (etwa Vermeiden unnötiger ad-hoc Listen und Aufstellungen, wenn sich die Information auch aus Quellen der normalen Tätigkeit gewinnen lässt), andererseits darf kein Bereich ungeprüft bleiben. Auch hier ist darauf zu achten, dass sensible Informationen geschützt bleiben müssen bzw. entsprechende Vertraulichkeitsvereinbarungen abgeschlossen werden. Dies gilt insbesondere auch für eingesetzte Prüfwerkzeuge. Solche dürfen nur von autorisierten Personen verwendet werden und sind selbst vor Missbrauch zu schützen.

Basis für die Prüfung sind primär Sicherheitspolitik, Sicherheitskonzept und dokumentierte Sicherheitsmaßnahmen. Selbstverständlich muss dafür gesorgt sein, dass das Management regelmäßig über Verlauf, Fortschritt, vorläufige Erkenntnisse und allfällige Probleme der Prüfung informiert wird.

Maßnahmen aufgrund der Prüfergebnisse:

Es ist vorab zu definieren, was aufgrund der Ergebnisse der Prüfung geschehen soll. Jedenfalls ist dem Management ein Prüfbericht vorzulegen:

- Was wurde jeweils im Einzelnen geprüft und von wem

- Was war die Prüfgrundlage (z. B. Sicherheitskonzept, Norm)
- Was war im Einzelnen das zu erreichende Prüfziel
- Inwieweit wurde es erreicht oder welche Abweichungen / Unregelmäßigkeiten wurden festgestellt
- War jeweils die Implementierung/Konfigurierung/Dokumentation korrekt
- Wie sind allfällig erkannte Schwachstellen/Unregelmäßigkeiten/neue Gefahren zu quantifizieren und welcher Handlungsbedarf ergibt sich daraus

Es ist dann die Pflicht des Managements, auf Basis der Ergebnisse entsprechende Verbesserungsmaßnahmen einzuleiten. Optimalerweise - bei regelmäßigen Prüfungen - existiert in der Organisation ein periodischer Verbesserungsprozess, im Rahmen dessen die Korrekturmaßnahmen dokumentiert, umgesetzt und ihrerseits wieder überprüft werden.

Verbesserungsmaßnahmen abhängig von der Ursache können sein:

- ISMS: Anpassung der Sicherheitspolitik oder des Sicherheitskonzepts
- Organisation: Abänderung organisatorischer Maßnahmen, zusätzliche Kontrollmechanismen, veränderte Zugriffsberechtigungen
- Personal: Awareness-, Schulungs- oder gar disziplinäre Maßnahmen
- Infrastruktur: Bauliche Veränderungen, veränderte Leitungsführungen
- Technik: Hard-, Softwareänderungen, Netzwerk-, Kommunikationsinfrastrukturanpassung

Zu jeder festgestellten Abweichung soll eine Verbesserungsmaßnahme vorgeschlagen werden - inklusive Zeitpunkt, Verantwortung und Ressourcen für ihre Umsetzung. Werden unzulässige Aktivitäten von MitarbeiterInnen entdeckt, sollte die/der jeweilige Vorgesetzte informiert werden, um angemessene Konsequenzen einzuleiten.

Schließlich entscheidet die Managementebene auf Basis der Prüfergebnisse, welche Konsequenzen zu ziehen bzw. Verbesserungsmaßnahmen einzuleiten sind. Dazu wird ein Umsetzungsplan verabschiedet, wobei festgehalten wird:

- Zeitaufwand und Fertigstellungstermine
- Verantwortlichkeiten für die Umsetzung
- Zur Verfügung gestellte Ressourcen

Die Umsetzung der Verbesserungsmaßnahmen ist dann Gegenstand des nächsten Audits.

[Quelle: BSI M 2.199]

18.1.2 Berichtswesen

Die Managementebene benötigt für ihre Entscheidungen aussagekräftige und aufbereitete Informationen. Dies gilt auch für die aktuelle Situation der Informationssicherheit. Um deren Niveau zu halten, ist dieses laufend zu bewerten und der Informationssicherheitsprozess zu steuern. Jede Änderung an den Sicherheitszielen, den Implementíerungen und im Umfeld wirkt sich auf das Sicherheitsniveau aus, daher muss die Managementebene darüber informiert werden.

Regelmäßige Managementberichte

Für die Managementebene sind nicht so sehr die Details, sondern die Eckdaten relevant:

- Ergebnisse von Audits und Überprüfungen
- Berichte von Not- oder Sicherheitsvorfällen
- Berichte über den Status des Informationssicherheitsprozesses (Erledigungen, Verzögerungen, Änderungen, Probleme, Ressourcenbedarf, künftige Planungen)
- Verbesserungsvorschläge

Dies sollte in regelmäßigen aber kurzen und übersichtlichen Berichten an die Managementebene erfolgen. Auf Aspekte, die bereits in anderen Berichten erörtert wurden, sollte ggf. verwiesen, diese aber nicht wiederholt werden. Die Sprache sollte auch für technisch nicht versierte Leser verständlich sein.

Ad-Hoc-Managementberichte

Im Anlassfall sollten Ad-hoc-Berichte erarbeitet werden, etwa:

- unerwartete Sicherheitsprobleme,
- neue Gefährdungspotenziale,
- neue Gesetze,
- Probleme die mit den vorgesehenen Ressourcen nicht gelöst werden können,
- in Massenmedien dargestellte Vorfälle - ob und inwieweit die eigene Organisation betroffen ist.

Abgesehen von bloßen Kenntnisnahmen ist das Ziel solcher Berichte meist eine Entscheidung der Managementebene. Diese wird nur dann erreicht, wenn zu den aufgezeigten Punkten auch klar formulierte Vorschläge für Maßnahmen dargestellt werden - inklusive einer Schätzung des damit verbundenen Aufwands bzw. Ressourcenbedarfs und der jeweiligen Priorität.

[Quelle: BSI M 2.200]

18.1.3 Einhaltung von rechtlichen und betrieblichen Vorgaben

Es ist dafür Sorge zu tragen, dass alle gesetzlichen und betrieblichen Vorgaben eingehalten werden.

Dazu ist laufend zu überprüfen,

- ob die Systeme allen gesetzlichen und betrieblichen Vorgaben entsprechen (insbesondere Beachtung neuer gesetzlicher Bestimmungen!) sowie
- ob die Vorgaben im laufenden Betrieb auch tatsächlich umgesetzt und eingehalten werden.

Wichtige Vorgaben ergeben sich beispielsweise aus:

- Datenschutzgesetz
- Einhaltung von gesetzlichen Aufbewahrungs- und Löschfristen
- Urheberrechtsgesetz und Wettbewerbsgesetze (etwa Verhindern von unbefugtem Kopieren von Software)

sowie

- Clear-Desk-Policy, falls vorgesehen (vgl. 7.1.7 Clear-Desk-Policy)
- Einhaltung von PC-Benutzungsregeln (vgl. 8.1.3.1 Herausgabe einer PC-Richtlinie)
- Einhaltung der Regeln für die Benutzung des Internets (siehe 14.7 Internet, Web, E-Commerce, E-Government)

18.1.4 Überprüfung auf Einhaltung der Sicherheitspolitiken

Vollständigkeit, Umsetzung, Einsatz sowie Einhaltung der Sicherheitspolitiken und -vorgaben sind regelmäßig zu überprüfen.

Es sollte regelmäßig überprüft werden,

- ob alle Sicherheitsmaßnahmen und -vorgaben, die in der organisationsweiten IT-Sicherheitspolitik sowie in den relevanten IT-Systemsicherheitspolitiken vorgesehen sind, vollständig und korrekt umgesetzt sind,
- der korrekte Einsatz der implementierten Sicherheitsmaßnahmen gewährleistet ist (Stichproben!) und
- die organisatorischen Sicherheitsvorgaben im täglichen Betrieb eingehalten und akzeptiert werden.

Diese Überprüfungen erfordern profundes Know-how über die zu prüfenden Systeme und die eingesetzten Sicherheitsmaßnahmen sowie mögliche Bedrohungen und sollten daher nur von erfahrenen und vertrauenswürdigen Personen durchgeführt werden.

18.1.5 Auswertung von Protokolldateien

> *Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind Protokolldateien in regelmäßigen Abständen durch RevisorInnen auszuwerten.*

Ist es technisch nicht möglich, die Rolle einer unabhängigen Revision für Protokolldateien zu implementieren, kann die Auswertung der Protokolldateien auch durch die Systemadministration erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten der Systemadministration nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher den Datenschutzbeauftragten/CISOs, den Applikations-/Projektverantwortlichen oder anderen besonders zu bestimmenden MitarbeiterInnen vorgelegt werden.

Die regelmäßige Kontrolle dient darüber hinaus auch dem Zweck, durch die anschließende Löschung der Protokolldaten ein übermäßiges Anwachsen dieser Dateien zu verhindern.

Beinhalten die Protokolldateien personenbezogene Daten, so ist sicherzustellen, dass diese Daten nur für die bei der Erhebung festgelegten Zwecke (beispielsweise Sicherstellung der Rechte der Betroffenen, der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes) verwendet werden dürfen (vgl. dazu Datenschutzgesetz und DSGVO).

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?

- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?

Weiters ist zu beachten:

- Müssen regelmäßig umfangreiche Protokolldateien ausgewertet werden, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfacher fehlerhafter Einlog-Versuch) hervorheben. Eventuell ist die Verwendung eines zentralen Log-Servers sinnvoll.
- Besonders sicherheitskritische Protokolldaten sollten unter Anwendung des Vier-Augen-Prinzips ausgewertet werden.
- Die Befugnisse der Systemadministration sind klar festzulegen; es ist dafür Sorge zu tragen, dass auch die Systemadministration ausreichend kontrolliert werden kann.
- Auffälligkeiten sind dem IT-Sicherheitsmanagement zu berichten (vgl. auch 16.1.3 Erstellung eines Incident Handling-Plans und Richtlinien zur Behandlung von Sicherheitsvorfällen)

18.1.6 Kontrolle bestehender Verbindungen

> *Alle Netzwerkkomponenten sind einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen.*

Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten/Veränderungen.

Neben der reinen Sichtkontrolle sollte zusätzlich eine funktionale Kontrolle durchgeführt werden. Dabei werden bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte hin geprüft. In zwei Fällen ist diese Prüfung anzuraten:

- bei Verbindungen, die sehr selten genutzt und bei denen Manipulationen nicht sofort erkannt werden,
- bei Verbindungen, auf denen häufig und regelmäßig schützenswerte Informationen übertragen werden.

Weiters ist zu beachten:

- Der Meldeweg für festgestellte Unregelmäßigkeiten ist festzulegen.
- Festgestellte Unregelmäßigkeiten müssen dokumentiert und verfolgt werden.
- Es ist festzulegen, wer für die Beseitigung von Unregelmäßigkeiten verantwortlich ist.

18.1.7 Durchführung von Sicherheitskontrollen in Client-Server-Netzen

Die folgenden Punkte sollten - abhängig von den Sicherheitsanforderungen und den technischen Möglichkeiten des betrachteten Systems - auf Serverebene regelmäßig auf Einhaltung und Effektivität kontrolliert werden.

- Systemsicherheitseinstellungen:
  Die Korrektheit aller sicherheitsrelevanten Systemeinstellungen ist regelmäßig zu kontrollieren.
- Benutzung von privilegierten Benutzeraccounts:
  Die Benutzung privilegierter Benutzeraccounts, also von Accounts mit erweiterten Rechten und Berechtigungen wie etwa der Systemadministration, ist regelmäßig durch Überprüfung der entsprechenden Protokolleinträge zu überprüfen.
- Fehlgeschlagene Zugriffsversuche (Berechtigungsverstöße):
  Sofern Zugriffe auf Dateien aufgezeichnet werden, ist das Protokoll zumindest wöchentlich, bei Bedarf auch öfter, auf das Vorliegen fehlgeschlagener Zugriffsversuche zu überprüfen. Werden Berechtigungsverstöße festgestellt, ist die Ursache zu ermitteln.
- Systemintegrität:
  Die Systemintegrität ist regelmäßig zu überprüfen; insbesondere sind die Daten der letzten Veränderung sowie die Zugriffsrechte der wichtigen Systemdateien zu überprüfen und mit den Werten, die unmittelbar nach der Installation des Systems sowie bei der jeweils vorherigen Überprüfung gegeben waren, zu vergleichen.
- Unbenutzte Benutzeraccounts:
  Es ist sicherzustellen, dass die Berechtigungen ehemaliger BenutzerInnen sofort deaktiviert und nach einer geeigneten Übergangszeit (ca. ½ Jahr) vom System gelöscht werden. Die Liste der definierten BenutzerInnen ist regelmäßig zu überprüfen, um sicherzustellen, dass nur aktive Beschäftigte auf dem System arbeiten.
- Benutzer- und Gruppenberechtigungen:

Es sollte überprüft werden, ob ProgrammiererInnen Zugriff auf Produktionsbibliotheken haben. Weiterhin ist die Gruppenmitgliedschaft zu überprüfen, wenn sich die Mitgliedschaft oder Aufgabe von BenutzerInnen ändert, und es sollte regelmäßig überprüft werden, ob Anhäufungen von Benutzerrechten existieren. Die Systemadministration sollte außerdem in regelmäßigen Abständen die BenutzerInnen mit Spezialberechtigungen mit den organisatorischen Vorgaben abgleichen.

- Berechtigungskontrolle:
  Es ist sicherzustellen, dass die EigentümerInnen von Dateien und Verzeichnissen ihre Verpflichtung verstehen, anderen BenutzerInnen nur dann Zugriff zu gewähren, wenn dies erforderlich ist.

Es sind Prozeduren bzw. Verfahren zu entwickeln für den Fall, dass Abweichungen von den festgelegten Einstellungen auftreten. Diese Prozeduren müssen folgende Punkte enthalten:

- wer wird wann informiert,
- Begründung für die eventuelle Wahl abweichender Einstellungen und Angabe, ob hierdurch möglicherweise eine Sicherheitslücke entsteht,
- Schritte zur Behebung der Sicherheitslücke,
- Schritte zur Identifizierung der Ursache der Sicherheitslücke.

18.1.8 Kontrollgänge

Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten ein einfaches und wirksames Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.

Die Kontrollgänge sollen nicht dem Suchen von TäterInnen dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässigkeiten möglichst sofort zu beheben (Fenster zu schließen, unbefugtes Offenhalten von Türen in Sicherheitsbereichen zu verhindern, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und evtl. in der Zukunft vermieden werden.

Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der MitarbeiterInnen über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

18.1.9 Fortlaufende Überwachung der IT-Systeme (Monitoring)

Monitoring ist eine laufende Aktivität mit dem Ziel, zu überprüfen, ob das IT-System, seine BenutzerInnen und die Systemumgebung das im IT-Sicherheitsplan festgelegte Sicherheitsniveau beibehalten. Dazu wird ein Plan für eine kontinuierliche Überwachung der IT-Systeme im täglichen Betrieb erstellt.

Wo technisch möglich und sinnvoll, sollte das Monitoring durch die Ermittlung von Kennzahlen unterstützt werden, die eine rasche und einfache Erkennung von Abweichungen von den Sollvorgaben ermöglichen. Solche Kennzahlen können beispielsweise die Systemverfügbarkeit, die Zahl der Hacking-Versuche über Internet oder die Wirksamkeit des Passwortmechanismus betreffen.

Da alle Änderungen der potenziellen Bedrohungen, Schwachstellen, zu schützenden Werte und Sicherheitsmaßnahmen möglicherweise signifikante Auswirkungen auf das Gesamtrisiko haben können, ist eine fortlaufende Überwachung dieser Bereiche erforderlich. Dies sind insbesondere:

Wert der zu schützenden Objekte

Sowohl die Werte von Objekten als auch, daraus resultierend, die Sicherheitsanforderungen an das Gesamtsystem können im Laufe des Lebenszyklus eines IT-Projektes oder -Systems erheblichen Änderungen unterliegen.

Mögliche Gründe dafür sind eine Änderung der IT-Sicherheitsziele, die Installation neuer Applikationen oder die Verarbeitung von Daten einer höheren Sicherheitsklasse auf existierenden (virtuellen) Systemen oder Änderungen in der HW-Ausstattung.

Bedrohungen und Schwachstellen

Organisatorisch oder technologisch (hier insbesondere durch neue Technologien in der Außenwelt) bedingt können sowohl die Wahrscheinlichkeit des Eintritts einer Bedrohung als auch die potenzielle Schadenshöhe im Laufe der Zeit starken Änderungen unterliegen und sind daher regelmäßig zu evaluieren.

Es ist wichtig, neue potenzielle Schwachstellen so früh wie möglich zu erkennen und abzusichern.

Sicherheitsmaßnahmen

Die Wirksamkeit der implementierten Sicherheitsmaßnahmen ist laufend zu überprüfen.

Es ist sicherzustellen, dass sie einen angemessenen und den Vorgaben der IT-Systemsicherheitspolitik entsprechenden Schutz bieten. Änderungen in den Werten der bedrohten Objekte, den Bedrohungen und den Schwachstellen, aber auch durch den Einsatz neuer Technologien, können die Wirksamkeit der Sicherheitsmaßnahmen nachhaltig beeinflussen.

Durch ein kontinuierliches Monitoring soll die Leitung der Institution ein klares Bild darüber bekommen, was durch die IT-Sicherheitsmaßnahmen erreicht wurde (Soll-/Ist-Vergleich), und ob die Ergebnisse den Sicherheitsanforderungen der Institution genügen. Weiters soll eine Beurteilung des Erfolges der einzelnen Maßnahmen erfolgen.

A.1 Sicherheitsszenarien

Dieser Anhang beschreibt gängige bzw. für Österreich spezifische Sicherheitsszenarien und -maßnahmen, die nicht Bestandteil der ISO 27000 Normenfamilie sind.

A.1.1 Industrielle Sicherheit

Im Zusammenhang mit Informationssicherheit werden unter dem Begriff „Industrielle Sicherheit“ Regelungen für den Umgang mit klassifizierten Informationen (das sind gemäß Informationssicherheitsgesetz EINGESCHRÄNKT, VERTRAULICH, GEHEIM, oder STRENG GEHEIM klassifizierte Dokumente) in Unternehmen bzw. in der Industrie verstanden. Diese Regelungen sehen unter anderem vor, dass die Sicherheit der betroffenen Unternehmen, Einrichtungen und Anlagen sowie ihres Personals im Rahmen einer so genannten Sicherheitsüberprüfung (Facility Clearance) überprüft wird.

Für die Teilnahme österreichischer Unternehmen an manchen Forschungsprogrammen wie zum Beispiel der Europäischen Weltraumagentur (ESA) ist die Vorlage solch einer staatlichen Bescheinigung erforderlich, wonach das Unternehmen und die Forschungseinrichtung die verlangten Standards der Geheimhaltung erfüllen (Sicherheitsunbedenklichkeitsbescheinigung).

Betroffen sind alle Unternehmen, welche Aufträge im Zusammenhang mit klassifizierten Informationen ausführen wollen bzw. sich an Ausschreibungsverfahren zu derartigen Aufträgen beteiligen wollen.

Im Rahmen eines Vertrages verpflichtet sich das Unternehmen die entsprechenden Rechtsvorschriften und internationalen Standards für die Behandlung klassifizierter Dokumente einzuhalten.

A.1.1.1 Beschreibung der generellen Anforderungen

Aufgrund der diversen rechtlichen Grundlagen müssen die Sicherheitsmaßnahmen

- alle Personen, die Zugang zu klassifizierten Informationen haben, die Träger von klassifizierten Informationen und alle Gebäude, in denen sich derartige klassifizierte Informationen und wichtige Einrichtungen befinden, umfassen;
- so ausgelegt sein, dass Personen, die aufgrund ihrer Stellung die Sicherheit von klassifizierten Informationen und wichtigen Einrichtungen, in denen klassifizierte Informationen aufbewahrt werden, gefährden könnten, erkannt und vom Zugang ausgeschlossen oder ferngehalten werden;

- verhindern, dass unbefugte Personen Zugang zu klassifizierten Informationen oder zu Einrichtungen, in denen klassifizierte Informationen aufbewahrt werden, erhalten;
- dafür sorgen, dass klassifizierte Informationen nur unter Beachtung des für alle Aspekte der Sicherheit grundlegenden Prinzips „Kenntnis nur wenn nötig“ (Need-to-know Prinzip) verbreitet werden;
- die Integrität (d. h. Verhinderung von Verfälschungen, unbefugten Änderungen oder unbefugten Löschungen) und die Verfügbarkeit (d. h. keine Verweigerung des Zugangs für Personen, die ihn benötigen und dazu befugt sind) aller Informationen gewährleisten.

Alle Gebäude, Bereiche, Büros, Räume, Kommunikations- und Informationssysteme usw., in denen als klassifiziert eingestufte Informationen oder ihr Material aufbewahrt werden oder in denen damit gearbeitet wird, müssen durch geeignete Maßnahmen des Geheimschutzes gesichert werden. Die Maßnahmen des Schutzes zielen darauf ab, das Eindringen unbefugter Personen von außen zu verhindern, von Tätigkeiten illoyaler Angehöriger des Personals (Spionage von innen) abzuschrecken bzw. diese zu verhindern und aufzudecken.

Im Wesentlichen werden dafür abgesicherte Sicherheitsbereiche eingerichtet und der Zugang zu diesen kontrolliert. Für die Lagerung von klassifizierten Informationen werden Sicherheitsbehältnisse (z. B. Tresore) vorgesehen. Weiters sind Maßnahmen zum Sicht- und Abhörschutz zu treffen. Außerdem ist zu dokumentieren, wann wer welche klassifizierte Information erhält. Die Gestaltung der Maßnahmen im Einzelnen ist von der Klassifizierungsstufe abhängig.

Personenzertifizierung

Alle Personen, die Zugang zu Informationen haben, welche als „VERTRAULICH“ oder höher eingestuft sind, müssen einer Sicherheitsüberprüfung unterzogen werden, bevor sie Zugangsermächtigung erhalten.

A.1.1.2 Rechtlicher Hintergrund

Rechtsgrundlagen

Als Rechtsgrundlagen sind zu nennen:

- Informationssicherheitsgesetz [InfoSiG]
- Informationssicherheitsverordnung [InfoSiV]
- Sicherheitspolizeigesetz [SPG]
- Militärbefugnisgesetz [MBG]
- Verordnung des Bundesministers für Verkehr, Innovation und Technologie über die Kostenersatzpflicht für die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung [BMVIT]

- Verordnung des Bundesministers für Landesverteidigung über die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen [SUBV]
- Sicherheitsgebühren-Verordnung [SGV]

Informationssicherheitsgesetz [InfoSiG] und –verordnung [InfoSiV] regeln den nationalen Umgang mit klassifizierten Informationen.

Für die Personenüberprüfung sind das Sicherheitspolizeigesetz [SPG] mit seinen Verordnungen, insbesondere die Sicherheitsgebühren-Verordnung und die Verordnung, mit der Form und Inhalt der Sicherheitserklärung einschließlich der Zustimmungserklärung erlassen und die Sicherheitsgebühren-Verordnung [SEV] geändert werden und das Militärbefugnisgesetz [MBG] relevant.

Die Verordnungen [BMVIT] und BMLV [SUBV] regeln die Kosten für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen.

Beschlüsse der ISK (Informationssicherheitskommission im Bundeskanzleramt):

- Beschluss über die Verwendung von Sicherheitsbehältnissen für klassifizierte Dokumente [TRES]

EU-Ratsbeschlüsse:

- Beschluss des Rates vom 19.03.2001 über die Annahme der Sicherheitsvorschriften des Rates (2001/264/EG) [EU2001]
- Beschluss des Rates vom 10.02.2004 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2004/194/EG) [EU2004]
- Beschluss des Rates vom 20.12.2005 zur Änderung des Beschlusses 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates (2005/952/EG) [EU2005]

Mit dem Ratsbeschluss 2001/246/EG [EU2001] wurde festgelegt, wie EU-Verschlusssachen in den öffentlichen Einrichtungen der Mitgliedsstaaten zu behandeln sind. Der materielle Geheimschutz wird definiert in Abschnitt IV: „Hauptziel der Maßnahmen des materiellen Geheimschutzes ist es, zu verhindern, dass Unbefugte Zugang zu EU Verschlusssachen erhalten.“

Im Ratsbeschluss 2004/194/EG [EU2004] werden die Anhänge 1 (Verzeichnis der nationalen Sicherheitsbehörden) und 2 (Vergleichstabelle der nationalen Sicherheitseinstufungen) des Ratsbeschlusses [EU2001] ergänzt.

Der Ratsbeschluss 2005/952/EG [EU2005] legt fest, dass die Bestimmungen des Ratsbeschlusses [EU2001] auch anzuwenden sind, wenn industrielle oder andere Einrichtungen vertraglich mit Aufgaben betraut werden, bei denen EU-Verschlusssachen relevant sind.

Beschlüsse der Kommission:

- Beschluss der Kommission vom 01.02.2005, 2001/844/EC, ECSC, Euratom in der sich diese inhaltlich an den Ratsbeschluss anlehnen
- Beschluss der Kommission vom 02.08.2006, 2006/548/EC, ECSC, Euratom hinsichtlich industrieller Sicherheit

Beschlüsse der NATO [NATO39]:

- [NATO] Security Committee, Directive on Industrial Security, „Security Policy“, AC735-D/2003-REV1, 26.07.2005 [NATO35]
- North Atlantic Council, C-M(2002)49, Security within the North Atlantic Treaty Organisation (NATO) mit den Subdokumenten [NATO49]
    - AC/35-D/2000 Directive on Personnel Security
    - AC/35-D/2001 Directive on Physical Security
    - AC/35-D/2002 Directive on Security of Information
    - AC/35-D/2003 Directive on Industrial Security
    - AC/35-D/2004 Primary Directive on INFOSEC
    - AC/35-D/2005 INFOSEC Management Directive for CIS

Beschlüsse der Multinational Industrial Security Working Group [MISWG]

- Doc. Number 1: Arrangements for the International Hand Carriage of Classified Documents, Equipment and/or Components
- Doc. Number 3: Use of Cryptographic Systems
- Doc. Number 4: Security Clauses
- Doc. Number 5: Program/Project Security Instruction
- Doc. Number 6: Procedures for the Protection of Restricted Information
- Doc. Number 7: International Visit Procedures
- Doc. Number 8: Controlled Unclassified Information Clauses
- Doc. Number 9: Security Education and Awareness
- Doc. Number 10: Transportation Plan for the Movement of Classified Material as Freight
- Doc. Number 11: Control of Security Cleared Facilities
- Doc. Number 12: Facility Security Clearance Information Sheet
- Doc. Number 13: Protection of Information Handled in it and Communication Systems
- Doc. Number 14: Contract Security Clauses
- Doc. Number 15: International Transportation by Commercial Carriers of Classified Documents and Equipment or Components as Freight
- Doc. Number 16: Guidelines for Assessing Protection and Control of Classified Information in a Multinational Non-NATO Cooperative Defence Program

- Doc. Number 17: International Hand Carriage of Classified Documents, Equipment and/or Components by Visitors
- Doc. Number 18: International Industrial Security Requirements Guidance Annex
- Doc. Number 19: Personal Security Clearance Information Sheet
- Doc. Number 20: International Transfer of Material Classified Restricted by Express Commercial Couriers
- Doc. Number 21: Role of the Facility Security Officer

A.1.1.3 Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung

Ablauf

- Anträge auf Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung sind beim zuständigen Ministerium einzubringen: Dabei handelt es sich um jenes Ministerium in dessen Zuständigkeitsbereich die betreffende industrielle Tätigkeit oder Forschungstätigkeit laut Bundesministeriengesetz fällt.
- Das Unternehmen verpflichtet sich gegenüber der Republik Österreich vertraglich zur Einhaltung der einschlägigen gesetzlichen Bestimmungen. Alle Personen, die im Unternehmen mit klassifizierten Informationen befasst werden sollen, sind gem. § 6 InfoSiV zu unterweisen. Die Nachweise der durchgeführten Unterweisungen sind an das zuständige Ministerium zu übermitteln.
- Personelle Sicherheitsüberprüfung (Personenzertifizierung): Alle Personen, die im Unternehmen Informationen erhalten sollen, welche als „VERTRAULICH“ oder höher (bzw. in einer äquivalenten ausländischen Klassifizierungsstufe) eingestuft sind, werden einer Sicherheitsüberprüfung unterzogen. Das Unternehmen beantragt eine Überprüfung für alle betroffenen MitarbeiterInnen. Die Sicherheitsüberprüfung wird gemäß §§ 55 bis 55 b SPG vom BMI oder im Falle der Zuständigkeit des BMLV die einer Sicherheitsüberprüfung analoge Verlässlichkeitsprüfung nach den §§ 23 und 24 [MBG] vom BMLV durchgeführt.
- Materielle Sicherheitsüberprüfung
    - Erstellen eines Sicherheitskonzeptes (inkl. der „Systemspezifischen Sicherheitsanforderungen“ [SSRS] für IT-Anwendungen) durch das Unternehmen
    - Umsetzen des Sicherheitskonzeptes und Dokumentation derselben (für IT-Anwendungen „SecOPs“ [SECOPS]) durch das Unternehmen
    - Überprüfung durch das BMI bzw. BMLV
- Ausstellung der Sicherheitsunbedenklichkeitsbescheinigung durch die/den LeiterIn der ISK bei zivilen Projekten bzw. die/den LeiterIn des Abwehramtes bei militärisch klassifizierten Projekten. Diese Bestätigung über die erfolgreiche Sicherheitsüberprüfung bezieht sich nur auf das konkrete Projekt, für welches die Überprüfung beantragt wurde und gilt für den angegebenen Zeitraum.

- In der Folge über die komplette Projektdauer: regelmäßige Überprüfung durch das zuständige Ministerium, Kommunikation mit dem Büro der Informationssicherheitskommission (ISK) z. B. bei Änderungen, Besuchsverfahren.

Verantwortlichkeiten und Kontakte

Antragstellung

Der Antrag auf Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung ist beim zuständigen Ministerium einzubringen. Dabei handelt es sich um jenes Ministerium in dessen Zuständigkeitsbereich der Auftragsgegenstand fällt. Unter http://www.austria.gv.at/ ist eine Liste der Ministerien zu finden. Bei Unklarheiten in der Zuständigkeit wird durch das ISK die Federführung festgelegt.

Durchführung der Sicherheitsüberprüfung und Ausstellung der Sicherheitsunbedenklichkeitsbescheinigung

- Büro der Informationssicherheitskommission (ISK), Bundeskanzleramt, Ballhausplatz 2, 1014 Wien
- Bundesministerium für Inneres, BVT/3, Herrengasse 7, Postfach 100, 1014 Wien
- Bundesministerium für Landesverteidigung, Abwehramt, Postfach 888, 1035 Wien

Durchführung der personellen Sicherheitsüberprüfung, Verlässlichkeitsprüfung

- Bundesministerium für Inneres, BVT, Herrengasse 7, Postfach 100, 1014 Wien
- Bundesministerium für Landesverteidigung, Abwehramt, Postfach 888, 1035 Wien

Verantwortlichkeiten im Unternehmen

Im Unternehmen sind eine Stelle (SOA - System Operational Authority) und eine verantwortliche Person (Informationssicherheitsbeauftragte/r) zu definieren, die für alle Sicherheitsmaßnahmen und für die Erstellung und Einhaltung der SSRS und der SecOPs verantwortlich sind.

Geheimhaltungsgrade und Kennzeichnungen

Österreich:	• STRENG GEHEIM (SG)	• GEHEIM (G)	• VERTRAULICH (V)	• EINGESCHRÄNKT (E)
EU Einstufung:	• TRES SECRET UE • EU TOP SECRET	• SECRET UE	• CONFIDENTIEL UE	• RESTREINT UE

NATO:	• Cosmic Top Secret	• NATO Secret	• NATO Confidential	• NATO Restricted

Tabelle A.1.1: Geheimhaltungsgrade und Kennzeichnung

Für einen kompletten Vergleich nationaler Sicherheitseinstufungen der EU-Mitgliedsstaaten, siehe Ratsbeschluss 2001/264/EG [EU2004] Abschnitt II.

A.1.2 Österreichische Strategie für Cyber Sicherheit (ÖSCS)

Mit der 2021 erneuerten Österreichischen Strategie für Cybersicherheit (ÖSCS) [OESCS] wurde von der Bundesregierung ein strategischer Rahmen für die nationale Cybersicherheitspolitik beschlossen. Die ÖSCS 2021 beruht auf den Grundsätzen der Österreichischen Sicherheitsstrategie (ÖSS) und ist eine Weiterentwicklung der ÖSCS 2013. Sie bildet das Fundament der gesamtstaatlichen Zusammenarbeit im Bereich der Cybersicherheit.

Mit der Österreichischen Strategie für Cybersicherheit wurde auf nationaler Ebene eine operative Cyberkoordinierungsstruktur festgelegt, die zur langfristigen Schaffung eines sicheren Cyberraums als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz beiträgt.

Die ÖSCS 2021 verfolgt dabei folgende Ziele:

- Österreich verfügt über ausreichende finanzielle und personelle Ressourcen, um Cyberbedrohungen und -vorfällen vorzubeugen, als solche zu erkennen, abzuwehren sowie derartige Angriffe strafrechtlich zu verfolgen;
- Österreich verfügt über die Fähigkeit, seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen und zu verteidigen;
- In Österreich wird Cybersicherheit als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat wahrgenommen; Verantwortlichkeiten und Zuständigkeiten sind klar definiert und werden von allen Beteiligten gelebt;
- Österreich verfügt über ein gesamtstaatliches Lagebild im Cyberbereich; Cybersicherheitskompetenzen werden in allen Gesellschafts-, Lebens- und Berufsbereichen gestärkt und gefördert sowie Awareness geschaffen;
- In Österreich ist eine sichere Partizipation am gesellschaftlichen und politischen Leben im Cyberraum für Bürgerinnen und Bürger möglich;
- Österreich hat klare gesetzliche und operative Möglichkeiten, um ein sicheres und attraktives Unternehmensumfeld im Cyberraum zu bieten und gegebenenfalls eine adäquate Strafverfolgung zu gewährleisten;
- Österreich engagiert sich aktiv im Cyberbereich und arbeitet intensiv mit allen Stakeholdern auf nationaler, europäischer und internationaler Ebene;

- Österreich kann im Zusammenwirken mit der EU seine digitale Souveränität gewährleisten und zur strategischen Autonomie der EU beitragen;
- In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit;
- Österreich bildet ausreichend viele Fachkräfte im Bereich Cybersicherheit aus, um die Resilienz im Bereich Cybersicherheit zu erhöhen, die Nachfrage des Arbeitsmarktes zu erfüllen und die Cyberkriminalität nachhaltig zu bekämpfen;
- Österreich leistet einen aktiven Beitrag bei der Anwendung und Stärkung internationaler Normen für den Cyberraum;
- Österreich arbeitet in einem gesamtstaatlichen Ansatz stetig an der Weiterentwicklung seiner Rechtsgrundlagen zur Erhöhung der Cybersicherheit und Bekämpfung der Cyberkriminalität.

Mit der konkreten Umsetzung der Maßnahmen im Maßnahmenkatalog (Kapitel 5 der ÖSCS) wird das Erreichen der Ziele verfolgt. Dadurch soll der sich ständig erweiternden Bedrohungslage sowie aktuellen Herausforderungen Rechnung getragen werden.

Bestehend aus hochrangigen Vertreterinnen und Vertretern mit Cybersicherheitsexpertise der im Nationalen Sicherheitsrat vertretenen Ressorts, verantwortet die Cyber Sicherheit Steuerungsgruppe (CSS) die Umsetzung der Strategie. Außerdem erstellt die CSS einen jährlichen Bericht zur Cybersicherheit und berät die Bundesregierung in Angelegenheiten der Cybersicherheit.

Essenziell für die Umsetzung der Strategie sind daher die konkreten Maßnahmen, die von den Ressorts selbst erstellt und in einem dynamischen Maßnahmenkatalog zusammengefasst werden. Dadurch soll der sich ständig erweiternden Bedrohungslage sowie aktuellen Herausforderungen Rechnung getragen werden. Die Strategie und ihre Umsetzung werden fortlaufend durch die Cyber Sicherheit Steuerungsgruppe (CSS) evaluiert und gegebenenfalls durch Maßnahmen auf Vorschlag der CSS und unter Einbindung der zuständigen Generalsekretärin bzw. des zuständigen Generalsekretärs ergänzt. Im Rahmen der Umsetzungsbeauftragung durch die Generalsekretärinnen bzw. Generalsekretäre erfolgt insbesondere auch die Sicherstellung organisatorischer, finanzieller und technischer Voraussetzungen.

A.1.3 Sicherheitsfunktionen für E-Government in Österreich

Auf EU-Ebene wird E-Government als „Einsatz der Informations- und Kommunikationstechnologien (IKT) in öffentlichen Verwaltungen in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten“ definiert, „um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern“. Der Begriff „E-Government“ (electronic Government) steht heute als Synonym für eine moderne und effiziente Verwaltung.

In der Folge werden wichtige Sicherheitsfunktionen des E-Government erörtert. Eine vollständige Betrachtung ist im „österreichischen E-Government ABC“ des Bundeskanzleramts zu finden.

E-Government in Österreich

Der Einsatz neuer Medien ermöglicht es den Behörden, Dienstleistungen über den traditionellen Weg hinaus einer breiten Öffentlichkeit zugänglich zu machen. Besonders das Internet hat zu einem qualitativen Fortschritt in der Kommunikation zwischen Amt und BürgerInnen beigetragen. Heute wird bereits eine Vielzahl an Informationen im Web angeboten. Die öffentliche Verwaltung geht schrittweise dazu über, alle Verfahrensschritte (Transaktionen) vom Antrag bis zur Erledigung eines Anbringens online anzubieten. Formulare brauchen in Zukunft nicht mehr heruntergeladen zu werden, sondern können gleich am Bildschirm ausgefüllt, elektronisch signiert und abgesendet werden. Erledigungen der Verwaltung, Bescheide und sonstige Schriftstücke müssen nicht mehr auf dem Postweg zugestellt werden. Sofern gewünscht, kann die Zustellung elektronisch erfolgen.

Im Rahmen der Neuausrichtung der IT-Strategie des Bundes wurde 2001 das IKT-Board, nun IKT-BUND genannt, eingerichtet. Das strategische Dach des E-Governments in Österreich bildet das Koordinationsgremium Plattform Digitales Österreich – PDÖ. Seine Aufgabe ist es, übergreifende Aspekte im Bereich der Informations- und Kommunikationstechnologien zu regeln sowie die Abstimmung mit Projekten auf Landes-, Gemeinde- und Städteebene vorzunehmen. Die Mitglieder der Plattform wurden jeweils von den Bundesministerien nominiert. Das Gremium IKT-BUND berät die Bundesministerin für Digitalisierung und Wirtschaftsstandort in allgemeinen Angelegenheiten der Informations- und Kommunikationstechnologie (IKT) bei der Besorgung ressortübergreifender IKT-Koordinationsaufgaben und bereitet die Durchführung von Strategischen Initiativen, die Erarbeitung/Beurteilung von Projektansätzen sowie die Definition und Festlegung

von Standards, Schnittstellen, Spezifikationen vor. Geleitet wird das Board vom „Chief Information Officer“ des Bundes, der der Bundesministerin für Digitalisierung und Wirtschaftsstandort kontinuierlich über seine Tätigkeiten berichtet. Die konkrete Durchführung der Projekte obliegt den Bundesministerien.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.1 ID Austria

Die sichere und zuverlässige Authentifizierung von Benutzerinnen und Benutzern über geeignete Anmeldeprozesse ist ein elementarer Baustein personalisierter Online-Anwendungen. Viele dieser Online-Anwendungen vertrauen dafür nach wie vor auf schwache Authentifizierungsmethoden, die etwa auf der Eingabe eines Benutzernamens und eines zugehörigen Passworts beruhen. Die diversen Nachteile solcher passwortbasierten Authentifizierungsmethoden in Bezug auf Sicherheit aber auch in Bezug auf Benutzerfreundlichkeit sind hinlänglich bekannt. Für Online-Anwendungen mit hohen Sicherheitsanforderungen, wie diese beispielsweise im Bereich des E-Governments zu finden sind, sind derartige Methoden der Benutzerauthentifizierung keine gangbare Alternative.

In Österreich und seiner E-Government-Infrastruktur standen mit Bürgerkarte und Handy-Signatur seit vielen Jahren benutzerfreundliche und zugleich auch sichere Alternativen für die Authentifizierung an Online-Anwendungen zur Verfügung. Sowohl Handy-Signatur als auch Bürgerkarte boten neben der sicheren und zuverlässigen Benutzerauthentifizierung Benutzerinnen und Benutzern seit jeher auch die Möglichkeit, elektronische Dokumente qualifiziert und damit rechtsgültig zu unterschreiben. Damit gewährleisteten Handy-Signatur und Bürgerkarte sowohl die Authentizität von Bürgerinnen bzw. Bürger gegenüber Online-Anwendungen als auch die Unveränderbarkeit signierter Daten und stellten seit vielen Jahren ein zentrales Element der österreichischen E-Government-Infrastruktur dar. Mit der Novelle zum österreichischen E-Government-Gesetz (EGovG) kommt es nun zu einer Weiterentwicklung von Bürgerkarte und Handy-Signatur zur sogenannten ID Austria, einem vollständigen elektronischen Identitätsnachweis.

Nationale und europäische gesetzliche Grundlagen als rechtliches Fundament der ID Austria

Rechtliche Grundlagen für die ID Austria sind neben dem novellierten E-Government-Gesetz und angrenzender Rechtsmaterien (z.B. Signatur- und Vertrauensdiensteverordnung - SVV) auch die Verordnung der Europäischen Union über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) sowie weitere Rechtsgrundlagen auf nationaler und EU-Ebene, die ebenfalls einen Einfluss auf Konzept und Umsetzung der ID Austria haben. Exemplarisch sei an dieser Stelle die Datenschutzgrundverordnung (DSGVO) in Verbindung mit dem Datenschutzgesetz (DSG) genannt, die entsprechend auch im Kontext der ID Austria zu berücksichtigen

ist. Die ID Austria fußt damit auf einem breiten rechtlichen Fundament, das zu weiten Teilen ihre Funktionen, konkrete Umsetzung und Eigenschaften definiert. Als vollständiger elektronischer Identitätsnachweis ermöglicht die ID Austria es Bürgerinnen bzw. Bürger, ihre Identität gegenüber Online-Anwendungen in gesicherter Form nachzuweisen. Durch ihre Konformität mit europäischen gesetzlichen Vorgaben soll die ID Austria nicht nur die Verwendung der persönlichen elektronischen Identität im Internet erleichtern, sondern darüber hinaus auch deren rechtliche Anerkennung in anderen europäischen Ländern sicherstellen.

Die ID Austria als Antwort auf geänderte Anforderungen und Nutzungsszenarien

Die bisher schon von Handy-Signatur und Bürgerkarte bekannten Nutzungsmöglichkeiten werden mit der ID Austria erweitert. So können Online-Anwendungen (sogenannte „Service-Provider“) künftig neben dem Namen und dem Geburtstag auch weitere Personenmerkmale (Attribute), wie zum Beispiel Einzelvertretungsbefugnisse, Führerschein- und Meldedaten, Staatsbürgerschaftsnachweise, etc. erhalten. Betroffene Benutzerinnen und Benutzer behalten dabei stets die Kontrolle über ihre Daten und können anlassbezogen entscheiden, ob sie der Übermittlung ihrer Attribute an den jeweiligen Service Provider zustimmen möchten.

Mit der Weiterentwicklung der bestehenden Lösungen Bürgerkarte und Handy-Signatur wird auch dem geänderten Nutzungsverhalten der Anwenderinnen und Anwender Rechnung getragen. Waren zum Zeitpunkt der Einführung von Bürgerkarte und Handy-Signatur klassische Endnutzergeräte wie Desktop-Computer und Laptops noch vorherrschend, ist mittlerweile ein klarer Trend hin zu mobilen Geräten wie Smartphones oder Tablets beobachtbar. Sowohl Bürgerkarte als auch Handy-Signatur sind in solchen mobilen Einsatzszenarien nur eingeschränkt verwendbar. Für die Bürgerkarte ist dies erkennbar, da die Verwendung von Chipkarten und entsprechenden Lesegeräten etwa auf Smartphones zwar prinzipiell denkbar, jedoch in jedem Fall wenig praktikabel. Überraschender mag klingen, dass auch die Handy-Signatur trotz ihres prinzipiell mobilen Charakters vordergründig für eine Verwendung auf klassischen Endgeräten ausgerichtet ist. Auch bei der Handy-Signatur kommt das mobile Gerät (Handy, Smartphone) als Zweitgerät im Zuge der Benutzerauthentifizierung zum Einsatz, der eigentliche Zugriff auf eine Online-Anwendung ist aber auch hier über ein klassisches Endnutzergerät vorgesehen. Die ID Austria ist hier flexibler und ermöglicht auch eine rein mobile Nutzung. Das bedeutet, dass ein und dasselbe mobile Gerät sowohl für den Zugriff auf Online-Anwendungen als auch für die Authentifizierung an dieser Anwendung verwendet werden kann. Unter anderem können so in Zukunft auch App-basierte Service-Provider die ID Austria nutzen, um beispielsweise Bürgerinnen bzw. Bürger innerhalb einer App zuverlässig über die ID Austria zu authentifizieren. Die Notwendigkeit der Verwendung eines klassischen Endnutzergeräts fällt mit der Einführung der ID Austria weg.

Sicherheit als zentrales Element der ID Austria

Die ID Austria stellt eine elektronische Identität für Bürgerinnen und Bürger dar und ermöglicht diesen einen sicheren Zugang zu Online-Anwendungen. Gleichzeitig bietet die ID Austria die Möglichkeit zur Erstellung rechtsgültiger elektronischer Signaturen. Dementsprechend ergeben sich für die ID Austria sehr hohe Sicherheitsanforderungen. Die Konzeptionierung, Umsetzung und Betrieb der ID Austria müssen einen Missbrauch bestmöglich verhindern. Die ID Austria beruht dazu auf erprobten Ansätzen und Lösungen, die sich bereits im jahrelangen Einsatz der Bürgerkarte und Handy-Signatur bewährt haben. Zusätzlich ergänzt die ID Austria diese Ansätze und Lösungen punktuell, um das Gesamtsicherheitsniveau weiter zu erhöhen. So werden die in modernen Smartphones verbauten sicheren Hardwarebausteine ebenso verwendet wie die von den mobilen Plattformen bereitgestellten sicheren biometrischen Authentifizierungsmethoden wie Fingerprint oder Gesichtserkennung. Dadurch kann eine gleichzeitige Verbesserung sowohl von Benutzerfreundlichkeit als auch Sicherheit erreicht werden. Für zentrale Komponenten der ID Austria wird das nötige hohe Sicherheitsniveau unter anderem durch deren Betrieb in sicheren und entsprechend zertifizierten Rechenzentren gewährleistet.

Die Eigenschaften der ID Austria im Überblick

Als Weiterentwicklung der Bürgerkarte bzw. Handy-Signatur erbt die ID Austria alle hervorzuhebenden Eigenschaften, die schon ihre Vorgängerlösungen ausgezeichnet haben. Durch gezielte Weiterentwicklungen und Verbesserungen wurden diese Eigenschaften noch um weitere Aspekte betreffend Funktion und Sicherheit erweitert. Im Folgenden sind die Kerneigenschaften der ID Austria zusammengefasst.

- **ID Austria als österreichisches nationales elektronisches Identitätsmanagementsystem.** Die ID Austria ist das österreichische nationale elektronische Identitätsmanagementsystem. Das bedeutet unter anderem, dass sämtliche elektronische Identitäten und die damit verknüpften Attribute auf Einträgen in den entsprechenden österreichischen staatlichen Registern beruhen. Für Online-Anwendungen ergibt sich damit eine hohe Sicherheit, dass die im Zuge von Authentifizierungsprozessen erhaltenen Benutzerattribute korrekt sind, dass also zum Beispiel der erhaltene Name tatsächlich jenem Namen entspricht, der für die Person in den entsprechenden Registern der österreichischen Verwaltung hinterlegt ist.
- **Aktualität von Attributen.** Die ID Austria stellt sicher, dass an Online-Anwendungen im Zuge von Authentifizierungsprozessen stets nur aktuelle Daten (sog. Attribute) ausgeliefert werden. Dies wird sichergestellt, indem die ausgelieferten Benutzerattribute im Zuge jedes Authentifizierungsprozesses erneut direkt aus den staatlichen Registern abgefragt werden.

- **Behördlicher Ausstellungsprozess.** Um die korrekte Zuordnung einer natürlichen Person zu ihrer elektronischen Identität (d.h. ihrer ID Austria) sicherzustellen, erfolgt der Registrierungs- und Ausstellungsprozess einer ID Austria für Bürgerinnen bzw. Bürger in behördlicher Qualität. Entsprechend befugte Behörden überprüfen im Zuge des Registrierungs- und Ausstellungsprozesses die Identität der Person und stellen so sicher, dass die Zuordnung von elektronischer Identität zur natürlichen Person korrekt und eindeutig ist.
- **Sichere Registrierungs- und Akkreditierungsprozesse für Service Provider.** Bürgerkarte und Handy-Signatur machten wenig Einschränkungen in Bezug auf ihre Verwendung durch Service-Provider (Online-Anwendungen). De facto konnte jede Online-Anwendung eine Benutzerauthentifizierung via Bürgerkarte und Handy-Signatur integrieren. Die ID Austria ist hier restriktiver. Nach wie vor steht die ID Austria prinzipiell allen Online-Anwendungen des öffentlichen und privaten Sektors offen, diese müssen sich jedoch zunächst registrieren, um an die Systeme der ID Austria angebunden zu werden. Für Service Provider des privaten Sektors ist zusätzlich ein Akkreditierungsprozess vorgesehen, über den unter anderem die Legitimität und Plausibilität der von der Online-Anwendung angeforderten Attribute, überprüft wird. Für Benutzerinnen bzw. Bürger ergibt sich damit zusätzliche Gewissheit, dass ihre Attribute nach erfolgter Zustimmung nur an legitime und entsprechend geprüfte Service-Provider ausgeliefert werden.
- **Grenzüberschreitende Einsatzmöglichkeiten.** Online-Anwendungen, die eine Benutzerauthentifizierung via ID Austria unterstützen, können damit automatisch auch Benutzerinnen und Benutzer über elektronische Identitätsmanagementsysteme anderer europäischer Länder authentifizieren. Dies ist darin begründet, dass die ID Austria in Zukunft über das europäische eIDAS-Interoperabilitäts-Framework mit Identitätsmanagementsystemen anderer Länder föderiert ist. Äquivalent dazu können Benutzerinnen und Benutzer, die über eine persönliche ID Austria verfügen, diese in Zukunft auch zur Authentifizierung an Online-Anwendungen anderer Länder verwenden.
- **Mehrfaktorauthentifizierung.** Der Nachweis der eigenen elektronischen Identität erfolgt stets über eine sichere Mehrfaktorauthentifizierung unter Ausnutzung der technischen Möglichkeiten moderner mobiler Endnutzergeräte. Online-Anwendungen können die konkrete Durchführung der Authentifizierung bis zu einem Grad abhängig von ihren Anforderungen beeinflussen. In die Authentifizierung gehen jedoch stets zumindest zwei Authentifizierungsfaktoren ein.
- **Qualifizierte Signatur als Zusatzfeature.** Die ID Austria bietet nicht nur eine sichere und zuverlässige Authentifizierung an Online-Anwendungen, sondern gibt Benutzerinnen und Benutzern zusätzlich auch die Möglichkeit der Erstellung qualifizierter elektronischer Signaturen. Die persönliche ID Austria kann damit beispielsweise zur rechtsgültigen Unterzeichnung von PDF-Dokumenten verwendet werden. Die beiden Features „Authentifizierung“ und „Signaturerstellung“ können prinzipiell getrennt voneinander verwendet werden.

Möglich ist darüber hinaus auch die Kombination beider Features innerhalb eines Verfahrens, das etwa Benutzerinnen bzw. Benutzern zunächst über deren ID Austria authentifiziert und diese im Anschluss zur Leistung einer rechtsgültigen elektronische Signatur auffordert.

- **Unterstützung von mobilen Nutzungsszenarien.** Im Gegensatz zu Bürgerkarte und Handy-Signatur unterstützt die ID Austria auch rein mobile Nutzungsszenarien, in denen zum Beispiel die Online-Anwendung über eine mobile App konsumiert wird und die Authentifizierung direkt an dieser App erfolgt. Die bei der Handy-Signatur bisher geltende Anforderung zur Verwendung zweier getrennter Endnutzergeräte wird durch die ID Austria obsolet.
- **Erweitertes Attribut-Set.** Im Vergleich zu Bürgerkarte und Handy-Signatur kann von der ID Austria an Online-Anwendungen ein erweitertes Set an Attributen ausgeliefert werden. Zusätzliche Attribute werden dabei aus zugänglichen Datenquellen (z.B. Verwaltungsregister) bezogen und ausschließlich nach Zustimmung der Benutzerinnen bzw. Benutzer an die anfragende Online-Anwendung im Zuge des Authentifizierungsprozesses ausgeliefert.
- **Nachhaltigkeit.** Informationstechnologien sind in einem hohen Maße laufenden Änderungen und Weiterentwicklungen unterworfen. Dies macht eine ständige Anpassung existierender Lösungen an geänderte Rahmenbedingungen und Anforderungen notwendig. Die über die ID Austria erfolgte Weiterentwicklung der etablierten Lösungen Bürgerkarte und Handy-Signatur ist ein Beispiel dafür. Die ID Austria in ihrer aktuellen Form darf hier jedoch keinen Schlusspunkt dieser ständigen Weiterentwicklung markieren, sondern muss ihrerseits ebenfalls laufend neuen Gegebenheiten angepasst werden. Um dies zu gewährleisten und effizient zu ermöglichen, wurde für die ID Austria eine nachhaltige und anpassungsfähige technische Architektur gewählt, die sich durch einen modularen Aufbau, eine einfache Anbindung von Service-Providern über Standard-Identitätsprotokolle sowie die Anbindung an den österreichischen Register- und Systemverbund auszeichnet.

Die oben im Überblick skizzierten Kerneigenschaften zeigen, dass die ID Austria auf den bewährten und erfolgreichen Konzepten von Handy-Signatur und Bürgerkarte aufbaut und diese weiterführt. Punktuell werden diese Konzepte an einigen Stellen gezielt weiterentwickelt und ergänzt, um aktuellen Anforderungen in Bezug auf Funktion und Sicherheit zu genügen.

Inbetriebnahme und Migration

Die ID Austria befindet sich derzeit in der Umsetzungs- und Pilotierungsphase. Anschließend ist die endgültige Produktivsetzung geplant. Bürgerinnen bzw. Bürger, die bereits über eine aktivierte Handy-Signatur verfügen, werden diese automatisch in eine persönliche ID Austria mit eingeschränkter Funktionalität, die im Wesentlichen jener der Handy-Signatur entspricht, überführen können. Zur Nutzung der vollen Funktionalität der ID Austria muss dann der vorgesehene Registrierungs- und Ausstellungsprozess bei einer befugten Behörde einmalig durchlaufen werden.

A.1.3.2 Konzept und Funktionen der Bürgerkarte

Das Konzept der Bürgerkarte stellt Funktionen für die Identifizierung und Authentifizierung bereit und besteht aus den im Folgenden beschrieben Elementen:

Bürgerkarten-Token

Der so genannte Token (zum Beispiel ein Chip auf einer Plastikkarte wie der e-card) ist das Element, welches die alleinige Kontrolle des Benutzers/der Benutzerin bei der Anwendung sicherstellt. Der Token löst die Berechnung von kryptografischen Funktionen und den Zugriff auf die Daten der Bürgerkarte aus. Die Daten auf der Bürgerkarte umfassen Namen, Vornamen und Geburtsdatum sowie die Schlüssel zur Signaturerstellung. In einem getrennt kontrollierten Bereich sind darüber hinaus die Stammzahl zur Ableitung der bereichsspezifischen Personenkennungen und, sofern eingerichtet, auch die Vertretungsdaten als signierte Daten nach den anwendbaren Standards vorhanden:

- Kryptografische Verfahren: Verschiedene mathematische Verfahren und Algorithmen finden bei der Erstellung von Signaturen Anwendung. Die Signaturverordnung 2008 regelt die gemäß dem sicherheitstechnischen Stand zulässigen Verfahren und Parameter.
- Schlüsselpaare für Signatur und Verschlüsselung: Zusätzlich zum Schlüsselpaar für die Erzeugung von qualifizierten elektronischen Signaturen laut Signaturgesetz ist auf Bürgerkarten in Form von Chipkarten in der Regel ein zusätzliches Schlüsselpaar für weitere Zwecke vorhanden. Dieses wird bei E-Government Verfahren nicht unbedingt benötigt und dient vor allem zur Datenverschlüsselung oder etwa zum Windows-Logon.
- Personenbindung: Im Bürgerkartenspeicher werden die Namen, das Geburtsdatum und die Stammzahl der Person durch die Stammzahlenregisterbehörde signiert gespeichert. Damit wird die Identität durch die Verwaltung bestätigt.
- Gegebenenfalls Vertretungsdatensätze: Diese binden die Stammzahl der vertretenden zur Stammzahl der vertretenen Person und beinhalten einen Index zum Widerruf der Vertretung, falls dies notwendig wird.

Aufgrund der Verwendung von offenen Standards können all jene Signaturkarten als Bürgerkarte verwendet werden, welche die im Rahmen der Bürgerkartenspezifikation und im Rahmen des rechtlichen Rahmenwerks festgelegten Anforderungen erfüllen.

Dies trifft auch auf ausländische „Bürgerkarten“ zu, also jene ausländische elektronische Identitäten, die auf Basis von elektronischen Signaturen gebildet werden (z. B. belgische elektronische Identitätskarten). Derartige elektronische Identitäten können unmittelbar als echte Bürgerkarten im österreichischen E-Government eingesetzt werden, sofern deren InhaberInnen die Ausstellung und

Eintragung einer Personenbindung (auf Basis eines ggf. durchzuführenden Eintrags im Ergänzungsregisters) beantragt und vorgenommen hat, sowie die Signaturkarte nach § 6 Abs. 5 E-Government-Gesetz als gleichwertig mit der Bürgerkarte anerkannt werden.

Anmerkung: Wegen der Umstellung auf die neue ID Austria („Funktion E-ID“ gem. § 4 E-GovG) können seit 31.12.2019 e-cards nicht mehr als Bürgerkarte aktiviert werden. Bereits als Bürgerkarte aktivierte e-cards behalten bis zum Auslaufen oder Widerruf des Signatur-Zertifikats bzw. bis zu allfälligem Austausch der Karte ihre Gültigkeit. Andere Karten (z.B. kommerzielle Smartcards) können weiterhin als Bürgerkarte aktiviert werden. Mit dem Wechsel auf den neuen elektronischen Identitätsnachweis ID Austria wird jedoch auf mobile Lösungen abgestellt, weshalb die Aktivierung der Handy-Signatur empfohlen wird.

Handy-Signatur

Die „Handy-Signatur“ (Bürgerkartenfunktion am Mobiltelefon) wurde von Österreich im Rahmen des EU-Großpilotprojekts zur Interoperabilität elektronischer Identitäten „STORK“ mit Unterstützung durch die EU-Kommission entwickelt und im vierten Quartal 2009 in Betrieb genommen. Die Lösung ermöglicht qualifizierte elektronische Signaturen mittels Mobiltelefon. Softwareinstallationen und zusätzliche Hardware (Kartenleser) sind im Gegensatz zur kartenbasierten Bürgerkarte (z. B. auf der freigeschaltenen e-card) nicht mehr nötig.

Bei Verwendung wird – ähnlich den von Banken für das E-Banking verwendeten Lösungen – nach erfolgter Anmeldung mittels Zugangskennung (Mobiltelefonnummer) und Passwort ein TAN-Code mittels SMS an das Mobiltelefon übermittelt. Die Eingabe dieses TAN-Codes in der jeweiligen Anwendung löst die qualifizierte elektronische Signatur aus. Mittels Mobiltelefon kann so auf denkbar einfache Weise eine qualifizierte elektronische Signatur erzeugt werden, die gleichwertig zur eigenhändigen Unterschrift nicht nur für elektronische Amtswege, sondern auch in der Privatwirtschaft – etwa beim E-Banking – uneingeschränkt Verwendung finden kann.

Es bestehen drei Möglichkeiten zur kostenlosen Aktivierung der Handy-Signatur:

- Die Aktivierung des Mobiltelefons zur Bürgerkarte kann sehr rasch mithilfe einer bestehenden Bürgerkarte (aktivierte e-card) über die Website www.handy-signatur.at des Vertrauensdiensteanbieters A-Trust erledigt werden.
- Eine weitere Möglichkeit der Aktivierung besteht darin, dass sich die NutzerInnen mit ihren herkömmlichen Login-Daten bei FinanzOnline anmelden und dort die Schaltfläche „Handy-Signatur aktivieren“ betätigen. Dieser Teil des Aktivierungsprozesses ist in wenigen Minuten erledigt. Etwa zwei Tage später erhalten die NutzerInnen per Papierpost einen Aktivierungscode, mit dem der Aktivierungsvorgang abgeschlossen wird

- Falls die NutzerInnen zu Hause keinen Internetanschluss haben sollten oder ein persönliches Beratungsgespräch bevorzugen, kann das Mobiltelefon in verschiedenen Registrierungsstellen, beispielsweise im „Servicezentrum HELP.gv.at“ am Ballhausplatz, als Bürgerkarte aktiviert werden. Eine Liste der Registrierungsstellen findet sich auf den Seiten des österreichischen Vertrauensdiensteanbieters A-Trust.

Wechsel auf die neue elektronische Identität ID Austria

Die ID Austria (wird gem. § 4 E-Government Gesetz als „Funktion E-ID“ bezeichnet) ist eine Weiterentwicklung der Bürgerkarte/Handy-Signatur und wird eine Erweiterung der Nutzungsmöglichkeiten sowie eine Änderung des Registrierungsprozesses mit sich bringen. Die Registrierung wird nur mehr behördlich erfolgen, so wird wer einen Reisepass beantragt, künftig automatisch eine ID Austria erhalten, außer dies wird ausdrücklich abgelehnt.

Im Zuge der geplanten Umstellung der Bürgerkarte/Handy-Signatur auf die neue ID Austria werden Service-Anbieter Schritt für Schritt an das neue System der ID Austria ankoppeln und Benutzerinnen und Benutzer im Anschluss über das System der ID Austria anmelden. Nach erfolgter Umstellung auf das System der ID Austria können sich Benutzerinnen und Benutzer vorerst weiterhin mit ihrer bestehenden Handy-Signatur oder Bürgerkarte anmelden.

Security Layer

Für die Umsetzung des Konzepts Bürgerkarte wurde der so genannte Security Layer spezifiziert. Dies ist die Schnittstelle zwischen der jeweiligen Applikation, also etwa einer Webanwendung, und der Signaturkarte und bietet Zugriff auf die Funktionen des Token zur Identifikation, Signatur und Verschlüsselung. Der Security Layer ist in die Software der Bürgerkartenumgebung (Middleware) eingebettet und erfüllt folgende Ansprüche:

- Unabhängigkeit von der eingesetzten Hardware und Technologie: Mit welchem Token die Signaturfunktion ausgeführt wird, ob auf einer Smartcard, einem USB-Stick oder als Web-Service soll für die Applikationen durch Anbieten einer logischen Sicht auf die Funktionalitäten unerheblich sein.
- Unabhängigkeit von den verwendeten kryptographischen Algorithmen: Da diese Verfahren durch den wissenschaftlichen und technischen Fortschritt mit der Zeit unsicher werden können, müssen sie ersetzt werden können, ohne dass Anwendungen von dem Wechsel beeinträchtigt werden.

Nach der Umstellung auf die neue ID Austria erfordert ein erfolgreicher Login dann eine aktive Handy-Signatur oder - bei Verwendung der Bürgerkarte - die aktuellste Version der A-Trust Bürgerkartenumgebung. Andere Bürgerkartenumgebungen wie zum Beispiel Mocca werden dann für Logins an Anwendungen, die bereits an das System der ID Austria angebunden sind, nicht mehr unterstützt.

Anzeige von Dokumenten und verwendete Formate

Wesentlicher Bestandteil einer Signaturlösung ist eine vertrauenswürdige Anzeige der zu signierenden Nachricht. Sie muss gewährleisten, dass keine für den Signator verborgenen Inhalte signiert werden können und auch keine dynamischen, den Inhalt nachträglich verfremdende Elemente zugelassen sind. So wird sichergestellt, dass zu signierende Inhalte (Texte, Formulare, Dokumente etc.) in jedem Fall auch beim Empfänger, der die Signatur prüft, identisch verarbeitet und dargestellt werden können. Um dies bei unterschiedlichen Implementierungen von Bürgerkartensoftware sicherzustellen wurde ein einheitlicher Standard für das Anzeigeformat entwickelt.

Die Basis für das Standardanzeigeformat bilden die internationalen Standards zur Darstellung von Webseiten „eXtensible HyperText Markup Language“ (XHTML) und „Cascading Style Sheets“ (CSS).

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.3 Personenkennzeichen und Stammzahlen

Elektronische Verfahren erfordern eindeutige Identifikationen von natürlichen oder juristischen Personen. Da dies keines der bisherigen Kennzeichen gewährleisten konnte, wurden für E-Government die in der Folge erörterten Personenkennzeichen eingeführt.

Das Konzept der Bürgerkarte stellt Funktionen für die Identifizierung und Authentifizierung bereit und besteht aus den Elementen:

Identifikationskennzeichen

- Stammzahlen natürlicher Personen
  Um Personen in elektronischen Verfahren eindeutig identifizieren zu können wird ein Merkmal benötigt, das eine Person eindeutig kennzeichnet. Da dies etwa für den Namen nicht zutrifft wird jeder Person ein künstliches Kennzeichen zugewiesen. In Österreich ist jede Bürgerin und jeder Bürger mit Wohnsitz im Inland unter einer „ZMR-Zahl“ im Zentralen Melderegister gespeichert. Da diese ZMR-Zahl besonderen rechtlichen Anforderungen unterliegt, kann sie jedoch nicht ohne weiteres zur Identifikation im E-Government herangezogen werden. Stattdessen wird die ZMR-Zahl mithilfe eines starken Verschlüsselungsverfahrens zur so genannten Stammzahl abgeleitet, welche nun auf der Bürgerkarte gespeichert werden darf und damit bestmöglichen Schutz sicherstellt. Die erhaltene 24-stellige alphanumerische Zeichenfolge darf einzig in der Bürgerkarte der BürgerInnen dauerhaft gespeichert werden. Das gesamte Verfahren der Ableitung der Stammzahl erfolgt durch die Applikation Stammzahlenregister für welche die Stammzahlenregisterbehörde verantwortlich ist. Der zur Ableitung verwendete geheime Schlüssel ist auch nur der Stammzahlenregisterbehörde bekannt.
- Stammzahlen nicht natürlicher Personen

Als Stammzahlen zur Identifizierung nicht natürlicher und juristischer Personen kommen je nach Rechtsform Firmenbuch-, Vereinsregister- oder Ergänzungsregisternummer zur Anwendung. Da diese Kennzeichen öffentliche Daten sind, werden sie in der Kommunikation im Klartext ohne Ableitungen verwendet.

Bereichsspezifische Personenkennzeichen

Da die Speicherung der Stammzahl nur in der Bürgerkarte erfolgen darf, sind zusätzliche Kennzeichen nötig, die im Rahmen eines behördlichen Verfahrens etwa in einer Datenbank gespeichert werden können. Zu beachten ist dabei, dass die Verwaltung in gesetzlich definierte Tätigkeitsbereiche untergliedert ist und nach dem E-Government-Gesetz in diesen Bereichen unterschiedliche Kennzeichen zum Einsatz kommen müssen. Aus der Stammzahl werden daher durch eine Einwegableitung bereichsspezifische Personenkennzeichen (bPK) gebildet, die wiederum nicht auf die Stammzahl rückführbar sind.

Die Behörde kann innerhalb eines Verfahrensbereichs nun die Daten der Bürgerin/ des Bürgers immer wieder unter demselben bPK finden und so zum Beispiel online Akteneinsicht oder vorausgefüllte Formulare unterstützen. Andererseits kennt eine Behörde aber weder bPKs anderer Bereiche noch die Stammzahl aus der diese bPKs berechnet werden könnten. Damit ist für den Schutz der persönlichen Daten des Einzelnen höchstmöglich vorgesorgt – eine wichtige Bedingung, um Vertrauen für die vielfältigen Möglichkeiten der elektronischen Dienste zu schaffen.

Verschlüsselte bereichspezifische Personenkennzeichen Verfahren der Verwaltung erfordern oft das Zusammenwirken von Behörden unterschiedlicher Bereiche, z. B. Bauwesen und Umweltschutz bei Errichtung einer Anlage oder eines Gebäudes. Es müssen daher Daten, die in den Bereichen unter verschiedenen bereichspezifischen Kennzeichen vorliegen, zusammengeführt werden können. Benötigt eine Behörde zur Identifikation einer natürlichen Person ein bereichsspezifisches Personenkennzeichen aus einem anderen Verfahrensbereich, kann dieses von der Stammzahlenregisterbehörde angefordert werden. Die Stammzahlregisterbehörde übermittelt das gewünschte bPK jedoch ausschließlich verschlüsselt und für diese unlesbar an die anfragende Behörde. Das bPK kann nur die Behörde entschlüsseln, die für den fremden Verfahrensbereich zuständig ist. Die Verschlüsselung des bPK muss so erfolgen, dass nicht auf die Person geschlossen werden kann und beruht auf asymmetrischer Verschlüsselung.

Personenkennzeichen für den privaten Bereich

Die Methode des aus der Stammzahl abgeleiteten bereichsspezifischen Personenkennzeichens zur Identifikation von Personen kann auch für den elektronischen Geschäftsverkehr mit der Privatwirtschaft verwendet werden.
Der Vorgang der Ableitung erfolgt analog zum bPK. Beim bereichsspezifischen Personenkennzeichen für den privaten Bereich wird jedoch anstelle der

Kurzbezeichnung eines Verwaltungsbereichs die Stammzahl jener juristischen Person verwendet, die etwa einen Kunden mittels bPK identifizieren will. Es wird also eine eindeutige Kennung erzeugt, die sich aus den Stammzahlen beider Kommunikationspartner zusammensetzt. Durch die Ableitung aus der geschützten Stammzahl wird auch im privaten Bereich gewährleistet, dass die Verwendung der bPK in privatwirtschaftlichen Anwendungen nur mit Wissen und Zustimmung der oder des Betroffenen erzeugt wird. Das bPK für Anwendungen der Privatwirtschaft wird unmittelbar von der Bürgerkartenumgebung am System des Benutzers/der Benutzerin aus der Stammzahl abgeleitet. Analog zu den Verwaltungsbereichen bildet so jedes Unternehmen oder jeder Verein auf Basis der Firmenbuch- bzw. Vereinsregisternummer einen eigenen Bereich.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.4 Vollmachten

Mithilfe elektronischer Vollmachten können Personen mit ihrer Bürgerkarte im Namen anderer Personen Verfahren durchführen.

Die vertretene Person kann dabei eine natürliche oder auch eine juristische sein. Zwischen natürlichen Personen kann dies der Fall sein, wenn BürgerInnen Online-Verfahren mittels Bürgerkarte nicht selbst abwickeln wollen oder können und diese Aufgabe jemanden – StellvertreterInnen – übertragen. Für juristische Personen ist es möglich, Verwaltungsverfahren durch eine berechtigte Person elektronisch durchführen zu lassen. Durch die elektronische Vollmacht kann die vertretene juristische Person eindeutig identifiziert werden.

Vollmachten werden im E-Government sowohl mit einer kartenbasierten Bürgerkarte als auch mit der Handy-Signatur umgesetzt. Für die Eintragung von Vertretungsbefugnissen auf der Bürgerkarte bzw. Handy-Signatur ist die Online-Anwendung Vollmachtenservice der Stammzahlenregisterbehörde vorgesehen. Im Ergänzungsregister für sonstige Betroffene, Firmenbuch oder Vereinsregister eingetragene Vertretungsbefugnisse werden automatisch vom Vollmachtenservice übernommen.

Die elektronische Vollmacht ist für Unternehmen besonders relevant, da die Bürgerkarte – sowohl bei der kartenbasierenden Variante als auch bei der Handy-Signatur – automatisiert gesetzliche Vertretungsverhältnisse abbilden kann, etwa für Prokuristinnen und Prokuristen bzw. für Geschäftsführerinnen und Geschäftsführer eines Unternehmens. Im konventionellen Geschäfts- bzw. Amtsverkehr bereits aufrechte Vertretungsverhältnisse werden elektronisch abgebildet. Das Unternehmensserviceportal (USP) dient als zentrale Drehscheibe der Online-Vollmachten sowohl für in das USP integrierte Verfahren als auch für den Zugang zu nicht in das USP integrierte Verfahren. Die Stammzahlenregisterbehörde fungiert dabei als Bindeglied zwischen dem Verfahren, das Vollmachten anfordert,

dem Unternehmensregister und dem Unternehmensserviceportal, das die Online-Vollmacht automatisiert zur Verfügung stellt. Über das USP können für das Unternehmen spezifische Vollmachten (z.B. für Zoll- und Importverfahren oder Postvollmachten) einem anderen Unternehmen oder einer natürlichen Person ausgestellt werden, mit dem Vertretungsmanagement im USP besteht die Möglichkeit, etwa 200 vorbereitete Vollmachten zu verwalten. Voraussetzung dafür ist lediglich, dass das Unternehmen im USP registriert ist. Sowohl die Verwaltung der Vollmachten als auch das Einschreiten der Bevollmächtigten kann einfach und praktisch mit der Handy-Signatur erfolgen.

[Quelle: Das österreichische E-Government ABC (BKA), oesterreich.gv.at]

A.1.3.5 Module für Online-Applikationen (MOA)

Die Module für Online-Applikationen (MOA) sind Softwarekomponenten, welche die Umsetzung bestimmter, von der E-Government-Strategie geforderter Funktionalitäten erleichtern, indem sie die dafür nötigen Prozeduren kapseln und Schnittstellen für Webapplikationen bereitstellen.

Zu den Funktionen gehören etwa die Prüfung und das Aufbringen von elektronischen Signaturen, das Auslesen der Identitätsdaten aus der Bürgerkarte oder die Zustellung von Schriftstücken der Behörden.

Die MOA waren von Beginn an dazu konzipiert, gemäß der E-Government Strategie Schnittstellen auf Basis offener internationaler Standards zu implementieren und lizenzkostenfrei zur Verfügung gestellt zu werden. Die zugrundeliegenden Spezifikationen wurden frei zugänglich veröffentlicht. Seit Juni 2005 sind die Module darüber hinaus quelloffene Software. Als Open-Source-Software kann der Quellcode der Module von jedermann eingesehen und weiterentwickelt werden.

Viele E-Government-Applikationen setzen inzwischen MOA ein und die Module sind unverzichtbarer Bestandteil geworden. Aus diesem Grund wird die Software in einem geregelten gemeinschaftlichen Prozess laufend gewartet und an neue Anforderungen angepasst. Zu diesem Zweck wurde eine eigene Plattform für die Entwicklergemeinde erstellt, auf der Änderungswünsche, Fehlerbereinigungen und Erweiterungen strukturiert eingearbeitet werden können. Auf der Plattform stehen die Module in allen Versionen inklusive Quelltext zur Verfügung.

Derzeit existieren Module für die Funktionalitäten:

- Identifikation (MOA-ID)
- Signaturprüfung (MOA-SP)
- Signaturerstellung am Server (MOA-SS)
- Zustellung (MOA-ZS)

- Amtssignatur (MOA-AS)

Im Folgenden wird auf diese Module eingegangen.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.5.1 MOA-ID (Identifikation)

MOA-ID ermöglicht die eindeutige Identifikation und sichere Authentifizierung von BenutzerInnen, die Online-Verfahren mit Bürgerkarte abwickeln. Identifizierung und Authentifizierung werden im Zusammenspiel des serverseitigen MOA mit der clientseitigen Bürgerkartensoftware durch die Personenbindung und die Signatur der Bürgerkarte durchgeführt.

Damit ist eine Anmeldung mit höchstem Sicherheitsniveau etwa für Akten- und Konteneinsicht, Banktransaktionen sowie generell für all jene Bereiche, in denen personenbezogene Daten gespeichert sind, möglich. MOA-ID bindet eine Session an benutzerspezifische Anmeldedaten aus der Personenbindung wie etwa das bereichsspezifische Personenkennzeichen, welches MOA-ID aus der Stammzahl der Bürgerkarte berechnet. Der Funktionsumfang von MOA-ID umfasst die Auswahl der Bürgerkartenumgebung, die Kommunikation mit dem Browser und der Bürgerkartenumgebung, die Authentifizierung und Identifizierung von BürgerInnen, Unternehmen oder Behördenvertretern mittels digitaler Signatur und Personenbindung, die Berechnung des bPK sowie die Weitergabe der Anmeldedaten an nachfolgende Applikationen. Alle dabei angezeigten Webseiten können im Erscheinungsbild an das Corporate Design der Organisation angepasst werden.

Nach erfolgter Authentifizierung fragt die nachfolgende Applikation die Anmeldedaten per Webservice oder Java-Programmierschnittstelle von MOA-ID ab. Alternativ kann auch eine Proxykomponente zwischengeschalten werden, welche die Anmeldedaten über zusätzliche Protokolle (z. B. als Parameter des HTTP-Headers) an solche Webapplikationen weitergibt, die weder Webservices noch interne Java-Aufrufe unterstützen. Die Proxykomponente ermöglicht so die unkomplizierte Einbindung der Authentifizierung mit der Bürgerkarte in bestehende Online-Applikationen. Allerdings sollten neue E-Government-Applikationen so aufgebaut sein, dass die Proxykomponente nicht benötigt wird.

Über das bereichsspezifische Personenkennzeichen für Wirtschaftsanwendungen ermöglicht das E-Government-Gesetz die Verwendung der Bürgerkarte auch für die Identifikation im Bereich der Privatwirtschaft. Die im Projekt MOA-WID entwickelten Erweiterungen zur Erzeugung und Nutzung von bereichspezifischen Personenkennzeichen durch private Personen wurden in die jüngsten Versionen von MOA-ID integriert.

Online-Verfahren der Verwaltung können auch von Dritten, so sie über eine gültige elektronische Vollmacht verfügen, stellvertretend für eine betroffene Person durchgeführt werden. Dafür wurde ursprünglich MOA-VV geschaffen, welches im Rahmen der Authentifizierung elektronische Vollmachten und Vertretungsregelungen verarbeiten konnte. Die Funktionalität von MOA-VV wurde ebenfalls in MOA-ID integriert.

Bei berufsmäßigen Parteienvertretern (z. B. Anwälten oder Zivilingenieuren sowie Organwaltern nach §5(3) E-GovG) zeigt eine standardisierte Erweiterung des Signaturzertifikats der Bürgerkarte den Umstand an, dass der Parteienvertreter in einem elektronischen Verfahren auch an Stelle eines Mandanten/einer Mandantin auftreten kann. Neben den Identitätsdaten des Vertreters/der Vertreterin, der/die sich mit Bürgerkarte anmeldet, ist MOA-ID in der Lage die Daten des/der Vertretenen zu ermitteln und an die Applikation weiterzureichen.

Im Gegensatz zur elektronischen Vollmacht, bei der die Daten der/des Vertretenen aus der XML-Struktur der Vollmacht ersichtlich sind, erfolgt die Identifikation des Mandanten/der Mandantin über die Eingabe von Attributen wie Name, Geburtsdatum und Geburtsort auf den Anmeldeseiten. Über ein Webservice des Stammzahlenregisters wird der Mandant/die Mandantin identifiziert und seine/ihre Anmeldedaten (z. B. das bPK) an MOA-ID zurückgesendet. MOA-ID übergibt die Daten wie auch bei einer Vollmacht an die nachfolgende Applikation.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.5.2 MOA-SP (Signaturprüfung)/MOA-SS (Signaturerstellung am Server)

MOA-SP / MOA-SS kapselt sämtliche Funktionalitäten der serverseitigen Signaturerstellung und -prüfung. Eine Signatur kann mittels Softwarezertifikat oder mit einem Hardware-Security-Modul erstellt werden.

Es werden Signaturen nach der XML-Signature-Spezifikation (XMLDSig) und bei der Prüfung auch nach Cryptographic Message Syntax (CMS) unterstützt, wobei es sich um einfache oder qualifizierte Signaturen handeln kann. Für die Signaturerstellung und -prüfung mittels Bürgerkartenumgebung muss der Prozess sowie die XML-basierten Anfrage- und Antwortnachrichten selbstverständlich konform zur Spezifikation Bürgerkarte sein.

Bei der Erstellung von Signaturen führt das Modul die Ermittlung des Signaturschlüssels, das Auflösen der zu signierenden Daten, Berechnung der Transformationen und die Erstellung der Signatur selbstständig durch. Es können auch Stapelsignaturen durchgeführt werden, wobei mit einem Auslösevorgang Signaturen auf mehreren Dokumenten erzeugt werden.

Wie auch bei MOA-ID können die Funktionen sowohl über SOAP-Webservices (Simple Object Access Protocol) als auch über eine Java-Programmierschnittstelle aufgerufen werden. Die Webservice-Schnittstelle bietet die Möglichkeit der sauberen Trennung zwischen aufrufender Applikation und MOA-Komponenten. Neben der Mandantenfähigkeit bietet dieses Design auch die Möglichkeit, Module zentral für mehrere Anwendungen zu betreiben.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.5.3 MOA-ZS (Zustellung)

MOA-ZS implementiert eine Schnittstelle zwischen Aktenbearbeitungssystemen bzw. Fachanwendungen und Zustelldiensten. Es führt selbstständig, und vor den BenutzerInnen verborgen, eine Reihe von Einzelschritten aus, die für die rechtmäßige und nachweisliche (elektronische) Versendung von Erledigungen notwendig sind.

MOA-ZS übernimmt im Rahmen der dualen Zustellung die Kommunikation mit dem Zustellkopf, die Ermittlung der Zustellungsart, das Aufbringen der Amtssignatur, die Inhaltsverschlüsselung von elektronischen Zustellstücken sowie die Übermittlung an eine Druckstraße oder einen elektronischen Zustelldienst. Die Empfangsbestätigung des Zustelldienstes an die Behörde wird ebenfalls durch die Webservices von MOA-ZS rückübermittelt.

Das Modul nimmt ApplikationsentwicklerInnen wesentliche Schritte bei der Abwicklung der Zustellung ab und soll so zu einer rascheren und kostengünstigeren Verbreitung der elektronischen Zustellung beitragen. Im Bund erfolgte bereits eine probeweise Umsetzung im elektronischen Akt (ELAK) und für Standardtextverarbeitungssoftware.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.5.4 MOA-AS (Amtssignatur)

Um für die elektronische Kommunikation von der Behörde zum Bürger auf das weit verbreitete Dokumentenformat PDF zurückgreifen zu können, müssen auch PDF-Dokumente mit einer Amtssignatur nach dem E-Government-Gesetz versehen werden können.

Das signierte Dokument enthält nach Aufbringen der Amtssignatur inkl. Bildmarke der Behörde die laut § 19 E-GovG zu visualisierenden Daten. MOA-AS stellt ein einfaches Webservice zur Verfügung um etwa PDF-Dokumente mit einer solchen Signatur, welche bei Bedarf auch vom Papierausdruck rekonstruiert und validiert werden kann, zu versehen.

Zum Aufbringen und Prüfen der PDF-Signatur ergänzt bzw. verwendet MOA-AS das Signaturmodul MOA-SS/SP, welches speziell für das Signieren von XML-Dokumenten entwickelt wurde und sich alleine daher nicht für die Amtssignatur eignet. MOA-AS soll es E-Government Applikationen ermöglichen Dokumente in gängigen Formaten wie bspw. PDF, Microsoft Word oder Open Document Format (ODF) amtssigniert in der Kommunikation mit BürgerInnen zu verwenden.

Die spezifizierte PDF-Signatur ist nicht nur für die Kommunikation mit der Verwaltung bestimmt, sondern kann auch im privaten Bereich zum Einsatz kommen. Damit können Bestellungen oder Rechnungen auf einfache Weise elektronisch unterschrieben werden.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.1.3.6 Portalverbund

Im Portalverbund können Datenanwendungen der Verwaltung anderen Behörden auf Basis einer gemeinsamen Nutzungs- und Sicherheitsvereinbarung und eines standardisierten technischen Portalverbundprotokolls (PVP) zugänglich gemacht werden.

Das Verbundsystem erlaubt teilnehmenden Organisationen, die eigene Benutzerverwaltung am sogenannten Stammportal auch für den Zugang zu Applikationen Dritter einzusetzen. Die BetreiberInnen dieser Anwendungen delegieren somit die Authentifizierung und Autorisierung einzelner BenutzerInnen an andere Portale. Anwendungsbetreiber legen nach den gesetzlichen Datenschutzbestimmungen nur zugriffsberechtigte Verwaltungseinheiten fest, nicht jedoch einzelne BenutzerInnen. Für diese definieren sie nur die möglichen Rollen. Die personalführenden Stellen vergeben die Rollen bzw. Zugangsrechte an die internen BenutzerInnen je nach Aufgabenstellung selbst. Als Vorteil ergibt sich ein

stark reduzierter Aufwand durch Entfall der Benutzerverwaltungen auf Seiten der Anwendungen. Das Führen paralleler Verzeichnisse ist somit nicht mehr notwendig. Auf Seiten der BenutzerInnen werden eine leichtere Handhabung und mehr Komfort durch Single-Sign-On ermöglicht.

Die Teilnahme von Verwaltungsorganisationen am Portalverbund wird durch die Portalverbundvereinbarung geregelt. Diese beinhaltet Rechte und Pflichten, die von den beigetretenen PortalverbundpartnerInnen einzuhalten sind, etwa BenutzerInnen bei der Anmeldung zu identifizieren oder weitere Datensicherheitsmaßnahmen umzusetzen. Dem Portalverbund können auch Gebietskörperschaften, sonstige Körperschaften des öffentlichen Rechts oder andere Institutionen, die staatliche Aufgaben besorgen, beitreten.

Das PVP stellt die technische Grundlage des Portalverbundes dar. In Ergänzung zur organisatorischen Portalverbundvereinbarung (PVV) werden im PVP technische Details der Übermittlung von Authentifizierungs- und Autorisierungsinformationen spezifiziert.

Dazu gehören etwa die Protokoll-Parameter, die Bindung an HTTP oder SOAP, die Portalarchitektur, Fehlermeldungen sowie URL-Konventionen. Der mittlerweile sehr erfolgreiche Portalverbund wurde auf der Basis bestehender technischer Ansätze definiert. Diesbezüglich wurde, auch bedingt durch die Kommunikation mit anderen Mitgliedstaaten, das schrittweise Anheben auf internationale Normen (z. B. SAML2) notwendig.

Im Portalverbund sind z. B. das Zentrale Melderegister, das Firmenbuch, das Zentrale Gewerberegister und die Grundstücksdatenbank verfügbar.

[Quelle: Das österreichische E-Government ABC (BKA)]

A.2 Sicherheitstechnologien

Dieser Anhang beschreibt gängige Sicherheitstechnologien unabhängig von der Struktur der ISO 27000 Normenfamilie.

A.2.1 Tunneling

A.2.1.1 Tunnelprotokolle für die VPN-Kommunikation

Tunneling bezeichnet das Verschlüsseln von Protokollverbindungen. Wird eine verschlüsselte Datenverbindung zwischen zwei Kommunikationspartnern aufgebaut, so realisiert diese Verbindung einen „sicheren Kanal“. Durch diesen Kanal können beliebige Daten sicher mit dem zugrunde liegenden Kommunikationsprotokoll (beispielsweise IP) übertragen werden. Stellen die übertragenen Daten selbst die Datenpakete eines Kommunikationsprotokolls dar, so spricht man auch von einem „Tunnel“.

Das Protokoll, das verwendet wird, um die Daten zu verschlüsseln, die verschlüsselten Daten durch den Tunnel zu übertragen und die Verbindung zu verwalten, wird auch als Tunnelprotokoll bezeichnet. Bei Tunnelprotokollen kann unterschieden werden,

- auf welchem Transport-Protokoll sie aufbauen und welcher Protokoll-Schicht (OSI-Layer) sie zuzuordnen sind,
- welche Protokolle über die Tunnel-Verbindung übertragen werden können,
- welche kryptographischen Verfahren zur Realisierung des Tunnels unterstützt werden,
- ob die Endpunkte des Tunnels authentisiert werden und
- ob über eine Verbindung des benutzten Transport-Protokolls der Aufbau mehrerer paralleler Tunnel möglich ist.

Das Tunnelprotokoll ist im Wesentlichen zuständig für

- Verwaltung des bzw. der Tunnel: Aufbau, Aufrechterhaltung und Abbau,
- Aushandeln der zu verwendenden kryptographischen Verfahren für die Realisierung des Tunnels: Schlüsselaustauschverfahren, Verschlüsselungsverfahren und Signaturverfahren,
- Ver- und Entpacken der Datenpakete der durch den Tunnel übertragbaren Protokolle sowie
- Ver- und Entschlüsseln der Datenpakete.

Bei der Wahl der eingesetzten Tunnel- bzw. VPN-Hard- und -Software sollte darauf geachtet werden, dass möglichst mehrere verschiedene und etablierte Verschlüsselungsverfahren unterstützt werden. Dadurch erhöht sich die Wahrscheinlichkeit, dass zwischen Client und Server geeignete Verfahren ausgehandelt werden können. Ein in der Praxis wichtiger Aspekt ist, dass die ausgewählten Tunnelprotokolle und die festgelegten kryptographischen Verfahren von allen beteiligten Tunnel-Endpunkten unterstützt werden müssen.

Übersicht über gängige Tunnelprotokolle

Im VPN-Umfeld haben sich folgende Tunnelprotokolle etabliert:

- *PPTP (Point to Point Tunneling Protocol):* Dieses Verfahren gilt seit einigen Jahren als unsicher und der Einsatz ist daher nicht zu empfehlen. PPTP ist ein Tunnelprotokoll auf Schicht 2. Es dient dazu, PPP-Verbindungen (Point to Point Protocol) über ein IP-Netz aufzubauen. Über die so hergestellte PPP-Verbindung können dann beispielsweise IP-Pakete transportiert („getunnelt“) werden. Die Sicherheitsfunktionen zur Authentisierung, Schlüsselverwaltung und Verschlüsselung werden von PPP bereitgestellt, häufig unter Nutzung des Microsoft Point-to-Point Encryption Protocol (MPPE). Im Sprachgebrauch wird jedoch oft nicht zwischen dem eigentlichen PPTP und der Kombination PPTP/PPP/MPPE unterschieden. In gängigen Implementierungen von PPTP wurden Sicherheitslücken entdeckt, insbesondere in Zusammenhang mit schwachen Passwörtern, wodurch die Verbindung keinerlei nennenswerte Absicherung mehr bietet. Ohne zusätzliche Sicherheitsmechanismen sollte PPTP daher nicht als VPN-Lösung eingesetzt werden bzw. generell von dessen Einsatz abgesehen werden.
- *L2TP (Layer 2 Tunneling Protocol):* Ähnlich wie PPTP dient L2TP in der Version 2 (L2TPv2) dazu, PPP-Verbindungen über paketvermittelte Netze aufzubauen. Im Gegensatz zu PPTP können bei L2TP jedoch neben IP auch andere Techniken als Trägernetz dienen, beispielsweise ATM. Für die Tunnel-Funktionalität nutzt L2TP dabei Mechanismen des von der Firma Cisco entworfenen Protokolls L2F (Layer 2 Forwarding). L2TP bietet selbst keine Funktionen zur Verschlüsselung der Datenpakete an. Eine solche Verschlüsselung muss entweder vom Trägernetz oder von den transportierten Protokollen geleistet werden. L2TP wird daher häufig in Kombination mit IPsec (siehe unten) eingesetzt.
- *IPsec (Internet Protocol Security):* IPsec ist ein Protokoll auf Schicht 3, das Funktionen zur Verschlüsselung und Integritätssicherung für IP-Kommunikation bietet. In Kombination mit dem IKE-Verfahren (Internet Key Exchange) kann auch ein automatisierter Schlüsselaustausch sowie eine Authentisierung der Tunnel-Endpunkte erfolgen. Ein manueller Schlüsselaustausch wird durch IPsec ebenfalls unterstützt. Die Authentisierung der BenutzerInnen muss jedoch über andere Verfahren erfolgen.

IPsec ist ein komplexes Protokoll, das mehrere unterschiedliche Optionen und Betriebsmodi bietet. Weiters sind die eingesetzten kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt, sondern es sind lediglich Mindestanforderungen aufgeführt. Beim Einsatz von IPsec muss daher im Rahmen der Konfiguration sichergestellt werden, dass die für den vorliegenden Anwendungsfall ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden.

- *TLS (Transport Layer Security):* TLS ist ein weit verbreitetes Verfahren, um Transportsicherheit beispielsweise für Web-Anwendungen oder E-Mail-Übertragung bereitzustellen. Einerseits können über TLS unterschiedliche Anwendungsprotokolle, wie z. B. HTTP, SMTP, POP3 oder IMAP, transportiert werden. Andererseits ist es mit Hilfe spezieller Softwarekomponenten auch möglich, IP-Tunnel über TLS aufzubauen. Aufgrund seiner Arbeitsweise lässt sich TLS nicht eindeutig einer bestimmten Protokollschicht zuordnen, häufig wird es jedoch als Schicht-4-Protokoll bezeichnet.
  TLS bietet Sicherheitsfunktionen zur Authentisierung und Verschlüsselung sowie zum Schlüsselaustausch und Integritätsschutz. Ähnlich wie bei IPsec sind die hierfür erforderlichen kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt. Vielmehr handeln die beteiligten Kommunikationspartner die verwendeten Verfahren beim jeweiligen Verbindungsaufbau aus. Es muss daher im Rahmen der Konfiguration sichergestellt werden, dass die ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden.
- *OpenVPN:* OpenVPN ist das gängigste Tunnelprotokoll und wird beispielsweise vom gleichnamigen VPN-Client verwendet. Es bietet je nach Betriebsmodus wahlweise eine Schicht 3 oder Schicht 2 Tunnelvariante. Das Protokoll ist quelloffen und unterstützt sowohl TCP- als auch UDP-Verbindungen. Die Verschlüsselung lässt sich durch die Verwendung der OpenSSL-Bibliothek frei konfigurieren (beispielsweise Blowfish oder AES), wodurch der Bedarf zwischen Sicherheit und Geschwindigkeit selbst gewählt werden kann.

Sonstige Tunnelprotokolle

VPN-Lösungen können nicht nur über die oben genannten Tunnelprotokolle, sondern auch über andere Verfahren aufgebaut werden. Ein Beispiel ist der Einsatz von (Open)SSH für VPN-Zwecke. SSH wurde primär als verschlüsselter Ersatz für telnet, ftp und die r-Dienste (rlogin, rsh, rcp, …) entwickelt, kann jedoch auch VPN-Verbindungen absichern.

Weiterhin werden Produkte am Markt angeboten, die proprietäre Tunnel- bzw. Verschlüsselungsverfahren nutzen. Der Einsatz proprietärer Verfahren sollte vermieden werden, da sich deren Sicherheitseigenschaften häufig nur schwer beurteilen lassen. Stattdessen sollten Verfahren eingesetzt werden, die sich an gängigen Standards und öffentlich verfügbaren Spezifikationen orientieren.

[Quelle: BSI M 5.76 Einsatz geeigneter Tunnelprotokolle für die VPN-Kommunikation]

A.2.2 Virtualisierung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Mehrere solcher Virtualisierungsserver können häufig zu einer virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet vielfältige Vorteile für den IT-Betrieb in einem Informationsverbund. Es können Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der Server effizienter genutzt werden. Durch die damit verbundene Zentralisierung und Konsolidierung sowie die vereinfachte Bereitstellung von IT-Systemen können im Bereich Personal und Administration ebenfalls Kostenvorteile erreicht werden. Die Möglichkeiten der Virtualisierung stellen aber auch gleichzeitig eine neue Herausforderung für den Betrieb des Informationsverbundes dar. Da durch den Einsatz der Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus den unterschiedlichsten Bereichen zusammengeführt werden.

A.2.2.1 Einführung in die Virtualisierung

Einführung in die Virtualisierung

Virtualisierung von IT-Systemen bezeichnet eine Technik, mit der ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben werden können. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Diese Technik wird bereits seit den 1970er Jahren bei den „Mainframes“ eingesetzt. Sie hat aber erst Ende der 1990er Jahre im Bereich der Midrange-Server weitere Verbreitung gefunden.

Die Virtualisierungstechnik hat sich sehr schnell als strategisches Mittel zur besseren Auslastung und Konsolidierung von Serversystemen durchgesetzt, da sie es ermöglicht, viele Dienste auf einem physischen Serversystem zu konzentrieren, ohne dass die Aufteilung der Dienste auf einzelne IT-Systeme aufgegeben werden muss. Dadurch werden die Ressourcen der physischen Server besser ausgenutzt und es können vielfach Einsparungen im Serverbetrieb erreicht werden. Diese Einsparungen beziehen sich nicht nur auf die Anzahl der einzusetzenden physischen IT-Systeme sondern auch auf die Stromkosten, den Platz in Serverräumen und Rechenzentren sowie die Klimatisierung. Weiters ist es möglich, durch die Virtualisierung Prozesse zur Bereitstellung neuer Server zu beschleunigen, da beispielsweise nicht für jedes neue Serversystem eine Bestellung durchgeführt werden muss. Bei einigen

Virtualisierungslösungen können virtuelle IT-Systeme kopiert werden, wodurch Installationsprozesse vereinfacht werden können, oder es können so genannte Snapshots von virtuellen IT-Systemen angelegt werden, die es ermöglichen, nach einer fehlerhaften Konfigurationsänderung schnell den ursprünglichen Zustand wiederherzustellen.

Mehrere Virtualisierungsserver können des Weiteren zu einer so genannten virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur werden mehrere Virtualisierungsserver gemeinsam mit den darauf laufenden virtuellen IT-Systemen verwaltet. Damit sind weitere Funktionen möglich. Beispielsweise können virtuelle IT-Systeme von einem Virtualisierungsserver auf einen anderen verschoben werden. Dies kann teilweise auch dann durchgeführt werden, während das virtuelle IT-System in Betrieb ist (Live-Migration). Weiters gibt es Möglichkeiten, die Verfügbarkeit der virtuellen IT-Systeme zu steigern. So können mittels der Live-Migration virtuelle Systeme immer auf den Virtualisierungsserver verschoben werden, der gerade die beste Performance für den Betrieb des virtuellen Systems zur Verfügung stellen kann. Eine weitere Möglichkeit besteht darin, virtuelle IT-Systeme automatisch auf einem anderen Virtualisierungsserver neu zu starten, wenn der ursprüngliche Virtualisierungsserver beispielsweise wegen eines Hardwaredefekts ausgefallen ist.

Die reichhaltigen Möglichkeiten zu Manipulation der virtuellen IT-Systeme durch die Virtualisierungssoftware lassen Virtualisierungsserver besonders für den Aufbau von Test- und Entwicklungsumgebungen geeignet erscheinen. Es ist mittels der Virtualisierung möglich, für Test- und Entwicklung schnell IT-Systeme bereitzustellen und komplexe Umgebungen schnell und effizient aufzubauen. Weiters können produktive virtuelle IT-Systeme für eine Test- und Entwicklungsumgebung kopiert werden, damit Aktualisierungen und Anpassungen ohne Störungen des Produktivbetriebes getestet werden können.

Voraussetzungen für den Betrieb virtueller IT-Systeme auf einem Virtualisierungsserver:

Um verschiedene virtuelle IT-Systeme auf einem Virtualisierungsserver sicher nebeneinander betreiben zu können, muss die Virtualisierungssoftware bestimmte Voraussetzungen erfüllen. Die Virtualisierungssoftware muss dafür sorgen, dass

- sich jedes virtuelle IT-System für die darin ablaufende Software nahezu wie ein eigenständiger physischer Computer darstellt (Kapselung),
- die einzelnen virtuellen IT-Systeme voneinander isoliert werden und nur über festgelegte Wege miteinander kommunizieren können (Isolation),
- die einzelnen virtuellen IT-Systeme in geordneter Weise auf die Ressourcen der Hardware zugreifen können.

Abhängig davon, wie die Virtualisierung der Ressourcen realisiert ist, werden diese Funktionen der Virtualisierungsschicht möglicherweise nur eingeschränkt erfüllt. So gibt es beispielsweise Lösungen, bei denen die Betriebssystem-Software leicht angepasst werden muss, bevor sie in einem virtuellen IT-System laufen kann. Ein anderes Beispiel für Einschränkungen bei der Virtualisierung sind Lösungen, bei denen alle virtuellen IT-Systeme auf einem Virtualisierungsserver verschiedene Instanzen des gleichen Betriebssystems verwenden müssen.

Die Virtualisierungsschicht muss nicht notwendigerweise eine reine Softwarekomponente sein. Bei einigen Plattformen unterstützt auch die Hard- oder Firmware die Virtualisierung der Ressourcen. Die Virtualisierungsschicht stellt den virtuellen IT-Systemen in der Regel konfigurierbare Zugriffsmöglichkeiten auf lokale Laufwerke und Netzverbindungen zur Verfügung. Dies erlaubt es den virtuellen IT-Systemen, miteinander und mit fremden IT-Systemen zu kommunizieren. In der Praxis werden zwei Arten von Virtualisierungssoftware unterschieden, die Servervirtualisierung und die Betriebssystemvirtualisierung.

[Quelle: BSI B 3.40Y]

A.2.2.2 Anwendungen der Virtualisierungstechnik

Mit Mitteln der Virtualisierungstechnik können einige Anwendungen entwickelt werden, die für physische Systeme in der Regel nur mit unverhältnismäßig hohem Aufwand realisiert werden könnten. Diese Anwendungen basieren in der Regel darauf, dass die Virtualisierungssoftware direkte Kontrolle über den Prozessor, den Arbeitsspeicher und die Massenspeicher des virtuellen IT-Systems hat. Sie kann direkt beeinflussen, wie diese Ressourcen durch das virtuelle System genutzt werden. Die Virtualisierungssoftware kann damit beispielsweise jederzeit den Zustand des Prozessors oder des Arbeitsspeichers des virtuellen IT-Systems auslesen. Diese Möglichkeiten können genutzt werden, um das virtuelle IT-System für unbestimmte Zeit einzufrieren. Weiters ist es möglich, in den Prozessor oder den Arbeitsspeicher zuvor gespeicherte Inhalte hinein zu laden. Der zuvor auf die Festplatte des Virtualisierungsservers gespeicherte Zustand von Prozessor und Arbeitsspeicher wird nach der Betriebsunterbrechung wieder geladen und die Ausführung der virtuellen Instanz wird genau an der Stelle fortgesetzt, an der das System eingefroren wurde. Dieses Verfahren ist nicht mit anderen Verfahren wie dem „Ruhezustand“ (Microsoft Windows) zu verwechseln. Im Gegensatz zum Ruhezustand geschieht diese Betriebsunterbrechung für das virtuelle IT-System völlig transparent. Die Möglichkeiten, ein virtuelles IT-System einzufrieren, werden genutzt, um so genannte Snapshots im laufenden Betrieb zu erzeugen.

Snapshots

Die meisten Virtualisierungslösungen ermöglichen das Konservieren des Zustands eines virtuellen IT-Systems zu einem beliebigen Zeitpunkt, ohne dass die Ausführung des virtuellen IT-Systems hierdurch beeinträchtigt wird. Beim Anlegen eines Snapshots wird die virtuelle Festplatte eingefroren und nachfolgende Schreibzugriffe werden in eine separate Datei umgeleitet. Der aktuelle Zustand ergibt sich bei Maschinen mit aktiven Snapshots aus der Überlagerung aller Snapshot-Dateien mit der Basis-Datei. Snapshots können mit oder ohne Inhalt des Arbeitsspeichers des virtuellen IT-Systems angelegt werden. Snapshots ohne Arbeitsspeicherinhalt spiegeln meist den Zustand des virtuellen IT-Systems wieder, das nicht heruntergefahren, sondern im laufenden Betrieb ausgeschaltet wurde. Snapshots mit Arbeitsspeicherinhalt erlauben es, das IT-System exakt in den Zustand zu versetzen, wie er zum Zeitpunkt des Snapshots vorlag, d. h., es ist eine Rückkehr in ein laufendes Betriebssystem mit geöffneten Anwendungen möglich. So lange der Snapshot nicht gelöscht wird, befindet sich der Speicherinhalt vom Zeitpunkt des Snapshots meist in Form einer Datei im Verzeichnis des virtuellen IT-Systems.

Live-Migration

Diese Techniken erlauben die Übertragung (Migration) von virtuellen IT-Systemen auf andere physische Virtualisierungsserver im laufenden Betrieb. Aus Benutzersicht, aber auch aus Sicht des virtuellen IT-Systems, geschieht dies unterbrechungsfrei. Hierdurch wird es z. B. möglich, Hardware eines Virtualisierungsserver zu erweitern oder auszutauschen, die Auslastung der Virtualisierungsserver gezielt neu zu verteilen sowie einen bestimmten Dienst oder eine Anwendung auf einen anderen Virtualisierungsserver zu verlagern.

Sowohl vor, während, als auch nach dem Migrationsvorgang muss der Zugang des virtuellen IT-Systems zum eigenen Dateisystem gewährleistet sein. Hierfür kommen Speichernetze (SAN-Systeme), die mittels Fibre Channel, iSCSI oder IP angebunden sind, und Netzdateisysteme (wie NFS) in Frage.

Diese Technik funktioniert im Wesentlichen so, dass zuerst ein Snapshot eines virtuellen IT-Systems vom Quell-Virtualisierungsserver auf den Ziel-Virtualisierungsserver übertragen wird. Der Zielserver lädt nun den Arbeitsspeicher des zu übertragenden virtuellen IT-Systems in seinen Speicher. Da das System auf dem Quellserver weiterläuft, hat sich der Speicher des virtuellen Systems in der Zwischenzeit verändert. Diese Änderungen werden nun fortlaufend übertragen und in Folge dessen wird das Zielsystem mit dem Quellsystem synchronisiert. Ist die Synchronizität hergestellt, wird das virtuelle IT-System auf dem Quellserver gestoppt, der Prozessorzustand auf den Zielserver übertragen und das virtuelle IT-System mit dem übertragenen Prozessorzustand auf dem Zielserver fortgesetzt. Dieser Vorgang erfolgt für das virtuelle IT-System vollständig transparent.

Die Live-Migration kann genutzt werden, um Performanceengpässen vorzubeugen. Dieser Prozess kann automatisiert werden, so dass jedem virtuellen IT-System immer die maximal mögliche Performance zur Verfügung gestellt werden kann.

Überbuchung von Arbeitsspeicher

Bei einigen Virtualisierungslösungen kann den virtuellen IT-Systemen in Summe mehr Arbeitsspeicher zugewiesen werden, als auf dem Virtualisierungsserver insgesamt vorhanden ist. Einem einzelnen virtuellen IT-System kann allerdings nicht mehr Speicher zugewiesen werden, als dem Hypervisor zur Verfügung steht. Ein Virtualisierungsserver verfügt beispielsweise über insgesamt zwei Gigabyte Hauptspeicher. Auf ihm werden drei virtuelle Server betrieben, die jeweils ein Gigabyte, also zusammen drei Gigabyte Hauptspeicher besitzen sollen. Um diese Überbuchung zu ermöglichen, wird den virtuellen IT-Systemen der entsprechende Hauptspeicher nicht zur Gänze zugeteilt. Stattdessen wird dem einzelnen virtuellen IT-System nur dann eine Speicherseite physisch zugewiesen, wenn sie von diesem virtuellen System tatsächlich gebraucht wird. Einmal durch ein virtuelles IT-System angeforderter Speicher kann grundsätzlich nicht durch den Hypervisor wieder zurückgefordert werden. So wächst der physische Speicherbedarf eines virtuellen IT-Systems sukzessive bis zur Konfigurationsgrenze an. Da allerdings davon ausgegangen werden kann, dass das Betriebssystem des virtuellen IT-Systems den ihm zur Verfügung stehenden Speicher mit der Zeit komplett nutzen wird, muss eine Möglichkeit bestehen, wie mit einer Ressourcensättigung auf dem Virtualisierungsserver umgegangen werden soll.

- Transparent Memory Sharing: Der Hypervisor überwacht alle Speicherseiten aller virtuellen IT-Systeme. Kann der Hypervisor zwei identische Speicherseiten identifizieren, werden diese nur einmal im physischen Arbeitsspeicher des Virtualisierungsservers vorgehalten. Ändert eines der virtuellen IT-Systeme eine dieser Seiten, wird sie für dieses System kopiert, und die anderen virtuellen IT-Systeme nutzen weiter die nicht modifizierte Seite. Diese Technik hat ein hohes Potenzial zur Speichereinsparung, da z. B. bei vielen virtuellen IT-Systemen die gleichen Betriebssystemkerne oder Softwarebibliotheken verwendet werden. Das Speicherabbild dieser Kerne oder Bibliotheken muss nur einmal physisch im Speicher des Virtualisierungsservers gehalten werden.
- Ballooning: In Abhängigkeit vom Hauptspeicherverbrauch des Gesamtsystems kann die Zuordnung von virtuellem Arbeitsspeicher zu den einzelnen virtuellen Systemen dynamisch angepasst werden. Möglich wird dies durch einen Treiber in dem virtuellen System, der gezielt Speicher belegt (Ballooning) und so das Betriebssystem des virtuellen IT-Systems zwingt, Hauptspeicherinhalte auf seine virtuelle Festplatte auszulagern. Der durch den Ballooning-Treiber belegte Speicher wird vom Server erkannt und kann an andere virtuelle IT-Systeme vergeben werden. Mittels dieses Verfahrens können Speicherengpässe kurzzeitig ausgeglichen werden. Da das Betriebssystem des virtuellen IT-Systems kontrolliert, welche Prozesse ausgelagert werden, ist der negative Performanceeinfluss meist kurzzeitig hinnehmbar.

- Paging: Kann der benötigte Speicher für ein virtuelles IT-System weder über Transparent Memory Sharing des Virtualisierungsservers noch über Ballooning im virtuellen IT-System freigegeben werden, wird der Speicher anderer, gerade nicht aktiver virtueller IT-Systeme durch den Hypervisor auf die Festplatten des Servers ausgelagert. Wenn dies geschieht, wird die Performance der virtuellen IT-Systeme sehr stark herabgesetzt, da der Hypervisor hier keine Rücksicht auf laufende Prozesse des Betriebssystems der ausgelagerten virtuellen IT-Systeme nimmt.

Überbuchung von Festplattenspeicher

Der Festplattenplatz des Virtualisierungsservers kann ebenfalls überbucht werden. Hierbei wird den virtuellen IT-Systemen mehr Festplattenplatz zur Verfügung gestellt, als tatsächlich vorhanden ist. Dabei wird der verfügbare Festplattenplatz so zugewiesen, dass die virtuelle Maschine ein Laufwerk mit beispielsweise einer Größe von zehn Gigabyte erkennt und ein Dateisystem von diesen Dimensionen anlegen kann. Auf der Festplatte des Virtualisierungsservers belegt das virtuelle IT-System jedoch nur den tatsächlich genutzten Platz in einer Containerdatei, die dynamisch mit der aktuell benötigten Speichergröße mitwächst. Sobald das virtuelle IT-System weiteren Platz nutzt, wird dieser auch auf der physischen Festplatte des Virtualisierungsservers belegt. Vom virtuellen IT-System freigegebener Speicher wird allerdings in der Regel nicht automatisch wieder physisch freigegeben.
Es muss weiters beachtet werden, dass die virtuellen IT-Systeme in eine Fehlersituation geraten, wenn der physische Speicher nicht mehr ausreicht, um weitere Speicheranforderungen zu erfüllen: Die virtuellen IT-Systeme „wissen“ nichts von der Überbuchung des Speichers und versuchen weiter auf ihre virtuellen Festplatten zu schreiben. Es kommt zu Schreibfehlern in den virtuellen IT-Systemen und in der Folge zu Inkonsistenzen im Dateisystem.

Fehlertoleranz für Hardwarekomponenten

Virtuelle IT-Systeme können bei einigen Virtualisierungsprodukten von Toleranzmechanismen bei Hardwarefehlern profitieren. Da die Virtualisierungssoftware die Zuordnung beispielsweise einer virtuellen Netzschnittstelle zu einer physischen steuert, kann die Kommunikation des virtuellen IT-Systems auf eine andere Netzschnittstelle umgeleitet werden, wenn die ursprüngliche Schnittstelle von einem Fehler betroffen ist. Stehen also in einem Virtualisierungsserver mehrere redundante Komponenten zur Verfügung, kann die Virtualisierungssoftware beim Ausfall einer Komponente für die Nutzung der noch funktionsfähigen Komponenten sorgen.

[Quelle: BSI B 3.40Y]

A.2.2.3 Gefährdungen in Zusammenhang mit Virtualisierung

Für den sicheren Betrieb von Virtualisierungsservern und virtuellen IT-Systemen gibt es aufgrund der vielfältigen Funktionen der Virtualisierungsserver und der Manipulationsmöglichkeiten für virtuelle IT-Systeme einige neue organisatorische und technische Gefährdungen.

Dies hängt damit zusammen, dass ein neuer Infrastrukturbestandteil, nämlich die Virtualisierungsinfrastruktur für IT-Objekte, entsteht. Auch können virtuelle IT-Systeme neue Zustände einnehmen. So kann sich ein System, das ausgeschaltet wurde, dennoch im Zustand laufend befinden, wenn es durch die Virtualisierungssoftware lediglich eingefroren wurde. Zudem werden Lebenszyklen von virtuellen IT-Systemen in der Regel in wesentlich kürzeren Zeitabständen durchlaufen.

In virtuellen Infrastrukturen werden die folgenden typischen Gefährdungen angenommen:

Organisatorische Mängel:

- Softwaretest mit Produktionsdaten,
- Unzureichende Leitungskapazitäten,
- Unkontrollierter Aufbau von Kommunikationsverbindungen,
- Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement,
- Fehlerhafte Planung der Virtualisierung,
- Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme,
- Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen,
- Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen.

Menschliche Fehlhandlungen:

- Fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ungeeignete Konfiguration der aktiven Netzkomponenten,
- Fehlinterpretation von Ereignissen,
- Fehlerhafte Zuordnung von Ressourcen des Storage Area Networks (SAN),
- Fehlerhafte Netzanbindungen eines Virtualisierungsservers,
- Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme,
- Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen,
- Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen.

Technisches Versagen:

- Ausfall von Diensten in einer virtualisierten Umgebung,
- Störung der Netzinfrastruktur von Virtualisierungsumgebungen,

- Ausfall von Verwaltungsservern für Virtualisierungssysteme,
- Ressourcenengpass durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen,
- Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse.

Vorsätzliche Handlungen:

- Unberechtigtes Kopieren der Datenträger,
- Unautorisierte Benutzung webbasierter Administrationswerkzeuge,
- Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes,
- Missbrauch von Virtualisierungsfunktionen,
- Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen,
- Kompromittierung des Hypervisors virtueller IT-Systeme.

[Quelle: BSI B 3.40Y]

A.2.2.4 Planung

Planung der virtuellen Infrastruktur

Aufgrund der hohen Komplexität ist eine detaillierte Planung beim Aufbau einer virtuellen Infrastruktur unerlässlich. Daher sollte schon bei einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung eine genaue Analyse der notwendigen Rahmenbedingungen durchgeführt werden.

In einem ersten Planungsschritt ist daher unter Berücksichtigung der für eine Virtualisierung infrage kommenden IT-Systeme festzulegen, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) die virtuelle Infrastruktur basieren soll. Hierbei sind im Wesentlichen folgende Kriterien heranzuziehen:

Die Servervirtualisierung, bei der ein vollständiger Server mit all seinen Hardwarekomponenten virtuell dargestellt wird, eignet sich besonders gut für den Betrieb von sehr unterschiedlichen virtuellen IT-Systemen mit stark variierenden Aufgaben. Bei Systemen auf der Basis einer Servervirtualisierung ist es möglich, unterschiedliche Betriebssysteme (Windows, Linux, Solaris) in den virtuellen IT-Systemen gleichzeitig auf einem Virtualisierungsserver zu betreiben, da jedes virtuelle System seinen eigenen Betriebssystemkern nutzen kann. Mit Hilfe der Servervirtualisierung kann eine sehr starke Kapselung der virtuellen IT-Systeme erreicht werden. Dies bedeutet, dass das virtuelle IT-System beispielsweise keine Betriebssystemkomponenten oder Softwarebibliotheken des

Virtualisierungsservers oder anderer virtueller IT-Systeme nutzt. Weiters sind bei der Servervirtualisierung die virtuellen Systeme stärker voneinander isoliert als bei der Betriebssystemvirtualisierung, d. h. eine wechselseitige funktionale Beeinflussung ist weitgehend ausgeschlossen.

Mittels der Betriebssystemvirtualisierung können auf einfache Weise große Mengen gleichartiger Server auf einem Virtualisierungsserver betrieben werden. Mit der Betriebssystemvirtualisierung können daher hohe Verdichtungsgrade (Verhältnis von virtualisierten IT-Systemen zu Virtualisierungsservern) erreicht werden. Es ist allerdings mit der Betriebssystemvirtualisierung in der Regel nicht möglich, unterschiedliche Betriebssysteme auf einem Server als virtuelle Systeme zu betreiben, da die virtuellen IT-Systeme meist den Betriebssystemkern und die Softwarebibliotheken des Virtualisierungsservers nutzen. In Grenzen ist dies bei einigen Produkten innerhalb einer Betriebssystemfamilie möglich. Die virtuellen IT-Systeme sind untereinander nicht so stark isoliert wie bei der Servervirtualisierung. Beispielsweise werden Softwarebibliotheken gemeinsam genutzt und die virtuellen IT-Systeme nutzen den selben Betriebssystemkern. Die Kapselung der virtuellen IT-Systeme ist meist gar nicht vorhanden oder nur sehr schwach ausgeprägt, da sie Soft- und Hardwarekomponenten des Virtualisierungsservers mit nutzen.

Diese schwache Kapselung der virtuellen IT-Systeme bei der Betriebssystemvirtualisierung führt dazu, dass virtuelle IT-Systeme mit stark unterschiedlichen Anforderungen an den Schutzbedarf nicht ohne Weiteres gemeinsam auf einem Virtualisierungsserver betrieben werden können. Dies ist bei Virtualisierungslösungen auf Basis einer Servervirtualisierung in der Regel anders, da die Kapselung der virtuellen Systeme stärker ausgeprägt ist. Ob allerdings virtuelle IT-Systeme mit unterschiedlichem Schutzbedarf auf einem Virtualisierungsserver zusammen betrieben werden können, hängt neben dem verwendeten Produkt auch von den individuellen Gefährdungen und Anforderungen der Organisation bzw. der virtuellen IT-Systeme ab. Daher ist bei der Planung zu bewerten, inwieweit die in Frage kommende Virtualisierungstechnik dafür geeignet ist, virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver gemeinsam zu betreiben.

Übergreifende Planung

Auf Virtualisierungsservern können eine Vielzahl von virtuellen IT-Systemen betrieben werden. Auf diesen virtuellen IT-Systemen, in der Regel Serversysteme mit unterschiedlichen Betriebssystemen, können weiters eine große Anzahl von verschiedenen Applikationen ausgeführt werden. Diese Applikationen wiederum benötigen in der Regel grundlegende Dienste wie DNS, Verzeichnisdienste zur Authentisierung oder Datenbanken. Daher müssen die Virtualisierungsserver auf alle Ressourcen zugreifen können, die für den Betrieb der Virtualisierungsserver selbst sowie der virtuellen IT-Systeme nötig sind. Die folgenden Anforderungen müssen bei der Planung eines Virtualisierungsprojektes beachtet werden. Die Virtualisierungsserver benötigen

- physische Verbindungen in alle Netze, in denen virtuelle IT-Systeme betrieben werden sollen.
- Verbindungen in Speichernetze zum Zugriff auf Massenspeicherkomponenten.
- Zugriff auf Infrastruktursysteme wie DNS-, DHCP- und Verzeichnisdienstserver.

Daher sollten alle Administratorengruppen, die mit der Bereitstellung dieser Dienste beauftragt sind, bei der Einführung der Virtualisierung angemessen beteiligt werden, damit diese ihre Kenntnisse einbringen und ihrerseits Anforderungen an das Virtualisierungsprojekt formulieren können.

Einsatzplanung für Virtualisierungsserver

Bei der Einsatzplanung ergeben sich Besonderheiten, weil auf einem Virtualisierungsserver in der Regel mehrere virtuelle IT-Systeme betrieben werden sollen. Es muss daher ermittelt werden, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz für den Betrieb der virtuellen IT-Systeme benötigt wird. Weiters muss festgelegt werden, welche Netzverbindungen für die Virtualisierungsserver und die virtuellen IT-Systeme benötigt werden.

Für die Auswahl geeigneter Virtualisierungsserver sind die Gesamtanforderungen bezüglich Performance und Ressourcenverbrauch für die geplanten virtuellen IT-Systeme zu ermitteln. Hierdurch erst kann die Anzahl und die benötigte Leistungsfähigkeit der Virtualisierungsserver festgelegt werden.

Bei einer Migration bereits produktiv betriebener physischer IT-Systeme in virtuelle Umgebungen sollte zudem der tatsächliche Ressourcenbedarf nicht einfach durch Addition der Ressourcen der zu virtualisierenden IT-Systeme ermittelt werden. Stattdessen empfiehlt es sich, die Performance der zu virtualisierenden Systeme zu messen und die Anforderungen an die Virtualisierungsserver auf Basis der erforderlichen Performancewerte der gemessenen physischen Server festzulegen.

Neben ausreichenden Ressourcen für die individuellen virtuellen Maschinen müssen darüber hinaus weitere Kapazitäten in der virtuellen Infrastruktur vorgehalten werden, die durch die Virtualisierungssoftware selbst benötigt werden. So entsteht ein zusätzlicher Bedarf an Massenspeicherkapazität etwa für die Speicherung von Snapshots, Ereignisprotokollen und Auslagerungsdateien des Virtualisierungsservers. Weiters benötigt der Hypervisor eines Virtualisierungsservers ebenfalls Prozessorkapazität und Hauptspeicherplatz. In Test- und Entwicklungsumgebungen kann von den obigen Vorgaben abgewichen werden.
Es ist bei der Planung solcher Umgebungen darauf zu achten, dass sich keine unerwünschten Wechselwirkungen mit Produktivsystemen ergeben. Daher sind Test- und Entwicklungsumgebungen hinreichend von Produktivumgebungen abzuschotten.

Verfügbarkeit der virtuellen Infrastruktur

Es wird empfohlen, in der Planungsphase schon zu berücksichtigen, dass für die Virtualisierungsserver möglicherweise höhere Anforderungen an die Verfügbarkeit bestehen, da auf Virtualisierungsservern eine große Zahl an IT-Systemen betrieben wird. Fällt ein Virtualisierungsserver aus, sind auch alle darauf laufenden virtuellen IT-Systeme nicht mehr lauffähig. Dadurch übertragen sich alle Verfügbarkeitsanforderungen der einzelnen virtualisierten IT-Systeme auf den Virtualisierungsserver (Kumulationsprinzip). Es ist ratsam, zu prüfen, ob für Virtualisierungsserver eine hochverfügbare oder fehlertolerante Architektur gewählt werden sollte, oder ob in einer aus mehreren Virtualisierungsservern aufgebauten virtuellen Infrastruktur Mechanismen existieren, die den Ausfall eines oder mehrerer Virtualisierungsserver kompensieren.

Auswahl eines Virtualisierungsproduktes

Ist die Virtualisierungstechnik ausgewählt, müssen konkrete Virtualisierungsprodukte geprüft werden, ob sie für den konkreten Anwendungsfall geeignet sind. Die hierbei zu berücksichtigenden Anforderungen leiten sich dabei aus den innerhalb der virtuellen Umgebung benötigten Prozessorarten sowie deren Funktionen und der Verfügbarkeit von erforderlichen Geräteemulationen oder Schnittstellen ab.

In einer möglichst frühen Planungsphase muss geprüft und entschieden werden, mit welcher Technik virtuelle IT-Systeme mit dem Netz des Rechenzentrums verbunden werden sollen: Entweder durch eine direkte Zuordnung von physischen Netzkarten des Servers zu den virtuellen IT-Systemen oder die Verbindung der virtuellen Systeme über einen so genannten virtuellen Switch. Auf dieser Basis kann festgelegt werden, wie Regelungen und Richtlinien umgesetzt werden können. Hierdurch ergeben sich schon frühzeitig Vorgaben für den Aufbau der Virtualisierungsserver und der dazugehörigen Infrastruktur. Sind die Anforderungen an die Zielumgebung geklärt, können eine passende Virtualisierungslösung und hierzu kompatible physische IT-Systeme ausgewählt werden.

[Quelle: BSI B 3.40Y]

A.2.2.5 Rollen und Verantwortlichkeiten bei der Virtualisierung

Da die Virtualisierungsserver häufig den Zugriff der virtuellen IT-Systeme und der darauf betriebenen Applikationen auf grundlegende Dienste des Rechenzentrums, sowie Netze und Speichernetze bereitstellen, sind sie aus der Sicht der virtuellen IT-Systeme selbst Bestandteil der Rechenzentrumsinfrastruktur. Daher wird empfohlen, für den Zugriff auf Netze und Speichernetze existierende Regelungen und Richtlinien an die Erfordernisse der virtuellen Infrastruktur anzupassen. Es sollte sichergestellt sein, dass diese auch innerhalb der virtuellen Infrastruktur umgesetzt werden können. Der Zugriff auf Speicherressourcen muss für die Virtualisierungsserver

möglicherweise weiter gefasst werden, da diese auf die Speicherressourcen vieler virtueller IT-Systeme zugreifen können müssen, damit sie wiederum selbst den virtuellen IT-Systemen Ressourcen zur Verfügung stellen können. Die Umsetzung muss jedoch mit den Mitteln der verwendeten Virtualisierungslösung möglich sein.

Dies zeigt, dass durch die AdministratorInnen der Virtualisierungsserver möglicherweise Aufgaben wahrgenommen werden müssen, die vorher durch die AdministratorInnen des Speichernetzes bzw. der Speicherkomponenten darin ausgeführt wurden. Gleiches gilt für die Aufgaben der Netzadministration. Die Verbindung von virtuellen IT-Systemen zu den unterschiedlichen Netzen des Informationsverbunds wird auf einem Virtualisierungsserver durch dessen AdministratorInnen festgelegt, da sie die virtuellen IT-Systeme den physischen Netzverbindungen des Virtualisierungsservers zuordnen. Dies ist traditionell eine Aufgabe der NetzadministratorInnen. Sollen auf einem Virtualisierungsserver virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden, muss die Verantwortung für die richtige Netzzuordnung und die Überwachung dieser Zuordnung durch die AdministratorInnen der Virtualisierungsserver übernommen werden. Zusätzlich muss berücksichtigt werden, dass das mit der Segmentierung des Netzes verfolgte Ziel, die Sicherheit durch Aufteilung der IT-Systeme auf verschiedene Bereiche des Rechenzentrums zu steigern, durch eine fehlende Kapselung und Isolation der virtuellen IT-Systeme auf dem Virtualisierungsserver nicht unterlaufen werden kann.

Es muss daher bei der Planung einer virtuellen Infrastruktur entschieden werden, wie die Aufgaben der Netz- und SpeichernetzadministratorInnen, falls bei der gewählten Virtualisierungslösung notwendig, von den AdministratorInnen der Virtualisierungsserver wahrgenommen werden sollen. Weiters ist zu prüfen, ob die Aufgaben der Verwaltung von Netz- und Speichernetzverbindungen durch die AdministratorInnen der Virtualisierungsserver an die Netz- und SpeichernetzadministratorInnen delegiert werden können. Die Betriebsverantwortung für die Umsetzung von bestehenden Regelungen und Richtlinien muss eindeutig und klar festgelegt werden.

[Quelle: BSI B 3.40Y]

A.2.2.6 Anpassung der Infrastruktur im Zuge der Virtualisierung

In klassischen Informationsverbünden sind IT-Systeme wie Server meist mit nur einem, seltener mit mehreren Netzen verbunden. Ein Virtualisierungsserver muss jedoch mit mehreren Netzen verbunden sein, wenn auf diesem Server virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden sollen. Daher ist die Umsetzung der Maßnahmen an die Besonderheiten und Erfordernisse der Virtualisierungsserver anzupassen.

Es muss darauf geachtet werden, dass die Virtualisierungsserver in einer virtuellen Infrastruktur alle Verbindungsanforderungen der virtuellen IT-Systeme erfüllen können.

Werden beispielsweise MAC-Filter (Media Access Control) auf Switch-Ports eingesetzt, muss die Konfiguration dieser Filter an die Erfordernisse der virtuellen Infrastruktur angepasst werden. Wenn das nicht der Fall ist, können virtuelle IT-Systeme, die bei einigen Virtualisierungslösungen eine eigene MAC-Adresse besitzen, nicht von einem Virtualisierungsserver auf einen anderen verschoben werden. Da diese Funktion möglicherweise für die Verteilung von virtuellen IT-Systemen auf Virtualisierungsserver benötigt wird, um auf Performance-Engpässe zu reagieren, ist ohne geeignete Anpassungen der Filterregeln die Verfügbarkeit von virtuellen IT-Systemen gefährdet.

[Quelle: BSI B 3.40Y]

A.2.2.7 Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern

Bei Virtualisierungsinfrastrukturen kommen zusätzlich zu den üblichen Rollen und Administrationstätigkeiten weitere administrative Aufgaben im Rechenzentrumsbetrieb hinzu. Die Besonderheit der Rolle von AdministratorInnen in einer virtuellen Infrastruktur besteht darin, dass diese potenziell eine sehr weitgehende Machtbefugnis über die virtuellen IT-Systeme, die in der virtuellen Infrastruktur betrieben werden, haben können.

Dies schließt mit ein, dass sie

- die Kontrolle über die emulierte Hardwareausstattung haben,
- die virtuellen IT-Systeme mit Netzen verbinden können,
- den virtuellen IT-Systemen Speicherressourcen aus dem Speichernetz zuweisen können und
- meist Zugriff auf die Konsolen der virtuellen IT-Systeme haben.

Eine Aufteilung der Administratorrolle ermöglicht die gegenseitige Kontrolle der unterschiedlichen Administratorgruppen in einem arbeitsteiligen Rechenzentrumsbetrieb. So können bei einigen Virtualisierungsprodukten, Administratorrollen definiert werden, die bestimmten Benutzergruppen eine Auswahl von Rechten in der virtuellen Infrastruktur zuweisen. Hier können beispielsweise bestimmte Benutzergruppen daran gehindert werden, virtuelle IT-Systeme aus der virtuellen Infrastruktur zu exportieren. Des Weiteren können Berechtigungen zum Ein- und Ausschalten von virtuellen IT-Systemen oder zur Erzeugung von Snapshots erteilt oder entzogen werden.

Es ist zu prüfen, ob für die virtuell zu betreibenden IT-Systeme eine Aufteilung der Administratorrollen notwendig ist. Dies kann beispielsweise der Fall sein, wenn eine bestimmte Administratorengruppe keine Berechtigung für die Zuweisung von Netzen für ein virtuelles IT-System mit erhöhtem Schutzbedarf bezüglich Vertraulichkeit erhalten soll.

Wird die Aufteilung der Administratorrollen benötigt, so ist die Definition entsprechender Administratorrollen für die Virtualisierungsinfrastruktur zu nutzen. Einige Virtualisierungsprodukte bieten eine solche Möglichkeit nicht. In diesem Fall ist zu prüfen, ob eine Aufteilung der Administratorrollen ausschließlich organisatorisch, das heißt z. B. mittels einer Richtlinie ausreicht.

[Quelle: BSI B 3.40Y]

A.2.2.8 Sichere Konfiguration virtueller IT-Systeme

Virtuelle IT-Systeme (meist auch als virtuelle Maschinen bezeichnet) sind in erster Linie IT-Systeme und daher genauso zu betrachten wie physische IT-Systeme. Allerdings gelten für virtuelle IT-Systeme einige Besonderheiten, die beachtet werden müssen. Virtuellen IT-Systemen muss oft der Zugang zu Geräten, die an den Virtualisierungsserver angeschlossen sind, wie beispielsweise DVD-Laufwerke, USB-Dongles, Bandlaufwerke und andere Peripheriegeräte, ermöglicht werden. Dabei können Geräte, die der Virtualisierungsserver den virtuellen IT-Systemen zur Verfügung stellt, häufig über Gastwerkzeuge aus der virtuellen Maschine heraus gesteuert werden. So kann beispielsweise die Netzwerkkarte deaktiviert werden oder es können Datenträger über das physische in das virtuelle BD-/DVD-Laufwerk geladen werden.

Bei einigen Virtualisierungssystemen besteht des Weiteren die Möglichkeit, Hauptspeicher oder Festplattenplatz zu überbuchen. Es wird von einer „Überbuchung“ von Ressourcen gesprochen, wenn den virtuellen IT-Systemen in Summe mehr Ressourcen zugewiesen werden können, als tatsächlich physisch vorhanden sind. Um Ressourcenengpässen vorzubeugen, können durch die Gastwerkzeuge in virtuellen IT-Systemen Funktionen bereitgestellt werden, um diese Überbuchungsfunktionen zu steuern. Die Gastwerkzeuge des Herstellers VMware (VMware Tools) besitzen beispielsweise eine Funktion, um Hauptspeicher zu belegen, der anderen virtuellen IT-Systemen zur Verfügung gestellt werden kann (Balooning). Diese Werkzeuge können auch eine virtuelle Festplatte für eine Verkleinerung des Dateicontainers, in dem sie enthalten ist, vorbereiten. Hierzu werden alle belegten Blöcke einer virtuellen Festplatte an den Anfang des Containers verschoben und die frei gewordenen Blöcke mit Nullen überschrieben, damit sie von der Virtualisierungsschicht als frei erkannt werden können.

Daher sind bei der Inbetriebnahme von virtuellen IT-Systemen neben den aus dem physischen Serverbetrieb schon bekannten Maßnahmen noch die folgenden Aspekte zu beachten:

- Veränderungen der Binärdateien von Kernel, Anwendungen und Systembibliotheken wirken sich bei der Betriebssystemvirtualisierung im Gegensatz zur Servervirtualisierung auf alle virtuellen IT-Systeme, die auf dem Virtualisierungsserver betrieben werden, sowie auf den Virtualisierungsserver selbst aus. Diese Daten sind auf Veränderungen hin zu überwachen, vor allem, da beispielsweise durch eine Kompromittierung solcher Dateien ein sehr hohes Schadenspotenzial entsteht.
- Die Gastwerkzeuge können es BenutzerInnen der virtuellen IT-Systeme ermöglichen, auf Datenträger in BD-/DVD-Laufwerken des Virtualisierungsservers zuzugreifen. Auch mechanische Vorgänge wie das Öffnen und Schließen der Laufwerksschublade eines physischen Laufwerkes können hierüber gesteuert werden. Es besteht daher die Möglichkeit, dass unberechtigt auf Datenträger in physischen Laufwerken zugegriffen wird, oder der Datenträger einem virtuellen IT-System entzogen wird, indem das Laufwerk von einem anderen virtuellen System aus geöffnet wird. Die virtuellen IT-Systeme und der Virtualisierungsserver müssen so konfiguriert sein, dass dies weitgehend ausgeschlossen ist. Am einfachsten kann dies geschehen, wenn den virtuellen IT-Systemen diese Geräte nur dann exklusiv zugeordnet werden, wenn sie aktuell benötigt werden. Werden sie nicht gebraucht, sollte die Verbindung zu diesen Geräten getrennt werden. Besteht die Möglichkeit, BD- oder DVD-Datenträger als Imagedateien (ISO-Images) statt über physische Laufwerke bereitzustellen, sollte sie genutzt werden.
- Funktionen, die die Überbuchung von Hauptspeicher oder Festplattenplatz ermöglichen, sind bei den virtuellen IT-Systemen zu deaktivieren, bei denen hohe Performanceanforderungen bestehen oder deren Datenintegrität besonders wichtig ist. Ressourcenengpässe bei einer Überbuchung von Hauptspeicher auf einem Virtualisierungsserver führen in der Regel zu starken Performanceeinbußen der davon betroffenen virtuellen IT-Systeme. Wird Festplattenplatz überbucht und reicht der physisch vorhandene Platz nicht mehr aus, werden durch den Virtualisierungsserver in der Regel keine weiteren Schreibzugriffe auf den überbuchten Speicherplatz zugelassen. Hierdurch treten in den virtuellen IT-Systemen Festplattenfehler auf, die zu Inkonsistenzen der abgespeicherten Daten führen können.
- Die Vorbereitung von virtuellen Festplatten auf eine Verkleinerung ihres physischen Containers bedeutet eine starke Belastung der Massenspeicher der Virtualisierungsserver. Dies kann zu Einschränkungen der Performance aller virtuellen IT-Systeme führen, die auf dem Virtualisierungsserver ausgeführt werden. Greifen mehrere Virtualisierungsserver auf ein Speichernetz zu, können unter Umständen alle Virtualisierungsserver davon betroffen sein. Daher sollte diese Funktion deaktiviert werden, wenn sie nicht benötigt wird.

- Die Deaktivierung von Geräten wie Netzwerkkarten über Gastwerkzeuge bildet ein virtuelles Äquivalent zur Entfernung des Netzwerkkabels eines physischen IT-Systems. Da dies in virtualisierten Umgebungen auch oft ohne Zutritt zu diesem System möglich ist, sollte diese Funktion deaktiviert werden. Sie sollte nur dann zeitweise aktiviert werden, wenn sie zwingend benötigt wird.

Einige der oben beschriebenen Funktionen werden über Gastwerkzeuge, die in den virtuellen IT-Systemen installiert werden können, gesteuert oder ermöglicht. Es sind daher verbindliche Regelungen zur Konfiguration und zum Einsatz dieser Gastwerkzeuge in virtuellen IT-Systemen zu erstellen.

- Die Integrität von Daten des Betriebssystemkerns, der Systembibliotheken und gemeinsam genutzten Anwendungen muss bei Umgebungen mit Betriebssystemvirtualisierungen gewährleistet sein.
- Es sind verbindliche Regelungen zum Einsatz von Gastwerkzeugen in virtuellen IT-Systemen zu treffen und umzusetzen.
- Externe Geräte wie USB-, BD-, DVD-Laufwerke sollen nur dann mit einem virtuellen IT-Systemen exklusiv verbunden werden, wenn sie im betreffenden IT-System benötigt werden.
- Für virtuelle IT-Systeme, bei denen hohe Performanceanforderungen bestehen oder ein hoher Schutzbedarf bezüglich Integrität festgestellt worden ist, sind Überbuchungsfunktionen für Hauptspeicher oder Festplattenplatz zu deaktivieren.
- Funktionen, mit der Geräte wie Netzwerkkarten oder externe Laufwerke über die Gastwerkzeuge aktiviert oder deaktiviert werden können, sollen standardmäßig ausgeschaltet werden.

[Quelle: BSI B 3.40Y]

A.2.2.9 Sicherer Betrieb virtueller Infrastrukturen

Auf Virtualisierungsservern werden in der Regel mehrere virtuelle IT-Systeme betrieben. Da die einzelnen virtuellen IT-Systeme allesamt von dieser Infrastruktur abhängen, kann ein Fehler auf einem Infrastruktursystem wie einem Virtualisierungsserver Auswirkungen auf sämtliche auf diesem System betriebenen virtuellen IT-Systeme haben.

Administrationszugänge

Virtualisierungsserver besitzen Funktionen, um die auf ihnen betriebenen virtuellen IT-Systeme zu steuern, zu warten und zu überwachen. Diese Verwaltungsfunktionen können in der Regel entweder lokal auf dem Virtualisierungsserver selbst oder über das Netz von der Arbeitsstation der AdministratorInnen aus genutzt werden. Dazu werden entweder webbasierte Administrationsoberflächen auf dem Virtualisierungsserver oder eine spezielle Administrationssoftware bereitgestellt.

Weiterhin besteht bei einigen Virtualisierungslösungen die Möglichkeit, mehrere Virtualisierungsserver sowie alle darauf betriebenen virtuellen IT-Systeme von einem zentralen System aus zu verwalten. Die entsprechenden Netzschnittstellen der Virtualisierungsserver bzw. des zentralen Verwaltungssystems ermöglichen einen vollständigen Zugriff auf die Virtualisierungsserver und die virtuellen IT-Systeme. Aus diesem Grund müssen die Administrationsschnittstellen abgesichert werden.

Überwachung des Betriebszustands

Die AdministratorInnen der virtuellen Infrastruktur sollten in regelmäßigen Abständen entsprechend der Sicherheitsrichtlinien Überwachungstätigkeiten ausführen. Hierzu gehört

- das Anlegen und das Löschen von Snapshots,
- die Überwachung des Betriebszustandes der Virtualisierungsserver und der virtuellen IT-Systeme,
- die Prüfung der Auslastung von Ressourcen,
- die Prüfung, ob ausreichend Prozessorressourcen zur Verfügung stehen, um die Performanceanforderungen der virtuellen IT-Systeme zu befriedigen,
- die Prüfung, ob Hauptspeicherengpässe bestehen, die die Verfügbarkeit der virtuellen IT-Systeme gefährden,
- die Prüfung, ob ausreichend Massenspeicher (Festplattenplatz bzw. zugeordnete und Gesamtkapazität im Speichernetz) zur Verfügung steht,
- die Prüfung, ob es Engpässe bei der Netzbandbreite gibt,
- die Prüfung der Verbindungen zu den physikalischen Netzen,
- der Integritätscheck der Konfiguration der Virtualisierungsserver und der virtuellen IT-Systeme.

Insbesondere dann, wenn die von einigen Virtualisierungsprodukten gebotene Möglichkeit zur Überbuchung von Hauptspeicher und Festplattenplatz genutzt wird, muss ein ständiger Prozess zur Überwachung dieser Ressourcen etabliert werden. Geschieht dies nicht, drohen im Fall von zu stark überbuchtem Hauptspeicher massive Performanceverluste. Wenn ein Engpass bezüglich des Festplattenplatzes entsteht, können alle davon betroffenen IT-Systeme gleichzeitig ausfallen. Wenn Snapshots verwendet werden, sollte die Auslastung des Massenspeichers ebenfalls sorgfältig beobachtet werden, da Snapshotdateien in der Regel dynamisch wachsen.

Die in regelmäßigen Abständen durchzuführenden Überwachungsaufgaben können in vielen Fällen automatisiert werden (z. B. E-Mail-Benachrichtigung etc.).

[Quelle: BSI B 3.40Y]

A.2.2.10 Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten

Der Ausfall von Virtualisierungsservern hat in der Regel weitreichende Folgen für den Informationsverbund. Dies liegt daran, dass nicht nur die Virtualisierungskomponente selbst von dem Ausfall betroffen ist, sondern auch alle virtualisierten IT-Systeme, die auf der Komponente betrieben werden.

Daher kann der Ausfall einer Virtualisierungskomponente nicht isoliert betrachtet werden. Es muss im Rahmen der Planung des Einsatzes der Virtualisierung von IT-Systemen im Rechenzentrum bedacht werden, dass durch die angestrebten Konsolidierungseffekte im Bereich des Hardwareeinsatzes auch das Schadensausmaß eines Ausfalls steigt. Dieses Schadensausmaß ist umso höher, je stärker sich die Konsolidierungseffekte auswirken. Daher muss der Schutzbedarf der Gesamtheit der virtuellen IT-Systeme auf den Schutzbedarf der Virtualisierungskomponenten abgebildet werden. Hierbei müssen das Maximumprinzip und das Kumulationsprinzip beachtet werden.

Es reicht des Weiteren häufig nicht aus, nur den Ausfall von Virtualisierungsservern, auf denen virtualisierte IT-Systeme betrieben werden, zu betrachten. Weitere IT-Systeme, die für den Betrieb der Virtualisierungsserver notwendig sind, müssen einbezogen werden. Der Ausfall dieser Systeme kann die Verfügbarkeit der Virtualisierungssysteme einschränken. Daher muss für die folgenden Systeme, falls vorhanden, eine Vorgehensweise bei ihrem Ausfall festgelegt werden:

- Virtualisierungsserver,
- Verwaltungsserver (insbesondere auch Connection-Broker),
- Netzwerkspeicher (SAN) und
- Lizenzierungsserver,

Je nachdem, wie die Virtualisierungssysteme in den Informationsverbund integriert sind, müssen auch weitere Systeme wie Verzeichnisdienste und Dienste zur Namensauflösung mit betrachtet werden. Da Infrastrukturdienste, wie Verzeichnisdienste oder Namensauflösungsdienste, auch auf virtualisierten IT-Systemen ausgeführt werden können, ist es möglich, dass sich durch den Ausfall einer oder mehrerer Virtualisierungskomponenten eine sehr komplexe Situation ergibt. So muss beispielsweise der Wiederanlauf eines stark virtualisierten Rechenzentrums wegen der sich hierbei häufig ergebenden Dienstabhängigkeiten detailliert geplant werden.

Folgende Aspekte müssen grundsätzlich berücksichtigt werden:

- Die Notfallplanung für Virtualisierungssysteme muss in den existierenden Notfallplan integriert werden.

- Durch einen Systemausfall eines Virtualisierungsservers kann es zu Datenverlusten in allen virtuellen IT-Systemen kommen, die auf dem ausgefallenen Virtualisierungsserver ausgeführt werden. Daher muss für alle virtuellen IT-Systeme geprüft werden, inwieweit die vorhandenen Datensicherungskonzepte an die gewählte Virtualisierungstechnik angepasst werden müssen. Es sollte für die virtuellen IT-Systeme geprüft werden, ob die neuen Techniken der Virtualisierung (Snapshots) zur Datensicherung genutzt werden können und welche Vor- und Nachteile sich hieraus ergeben könnten. Wichtige Images müssen in die Datensicherung einbezogen werden.
- Fällt ein Virtualisierungsserver aus, so fallen alle darauf laufenden virtuellen IT-Systeme ebenfalls aus. Die Wahrscheinlichkeit, dass es bei mindestens einem betroffenen virtuellen IT-System zu einem ernsthaften Datenverlust kommt, steigt mit der Anzahl der betroffenen Systeme. Es ist also bei der Notfallplanung zu berücksichtigen, dass möglicherweise ein umfangreicherer Wiederherstellungsaufwand eingeplant werden muss.
- Werden mehrere Virtualisierungsserver in einer Farm eingesetzt (virtuelle Infrastruktur), ist darauf zu achten, dass eine sinnvolle Gruppierung der virtuellen IT-Systeme gewählt wird. So sollten beispielsweise zwei Systeme, die wechselseitig die Aufgaben des jeweils anderen ausführen können, nicht auf einem Virtualisierungsserver betrieben werden.
- Es muss sichergestellt werden, dass im Notfall für den Umgang mit virtuellen Infrastrukturen geschultes Personal zur Verfügung steht.
- Die Systemkonfiguration der Virtualisierungsserver muss für die AdministratorInnen jederzeit einsehbar sein. Sie muss so gestaltet sein, dass die Virtualisierungsserver im Notfall auch von Personal wiederhergestellt werden können, das mit der vorher vorhandenen Konfiguration nicht detailliert vertraut ist.
- Es muss ein Wiederanlaufplan erstellt werden, der den geregelten Neustart der Virtualisierungsserver und der mit ihm ausgefallenen virtuellen IT-Systeme gewährleistet.
- Es muss sichergestellt sein, dass die Wiederinbetriebnahme der Virtualisierungssysteme nicht von einem Dienst im Rechenzentrum abhängt, der ausschließlich von einem virtuellen IT-System bereitgestellt wird. Im Rahmen der Notfallvorsorge sollten unterschiedliche Szenarien betrachtet werden, in dem die Virtualisierungssysteme ganz oder in Teilen kompromittiert worden sind. Für diese Szenarien ist präzise zu beschreiben, wie hierauf zu reagieren ist und welche Aktionen jeweils auszuführen sind. Die Vorgehensweise sollte regelmäßig geübt werden.

Eine rechtzeitige Notfallplanung mit vorgegebenen Handlungsanweisungen, die auch von Personen ausgeführt werden können, die nicht detailliert mit der Administration der Virtualisierungssysteme vertraut sind, kann die Folgen im Schadensfall verringern. Die entsprechenden Dokumente für Notfallsituationen müssen für berechtigte Personen zugreifbar sein. Da sie allerdings wichtige Informationen beinhalten, müssen sie geschützt aufbewahrt werden.

Angriff

Wurden Angriffe auf die Virtualisierungssysteme entdeckt, kann nicht davon ausgegangen werden, dass diese auf die Virtualisierungssysteme selbst begrenzt waren. Es muss vielmehr geprüft werden, ob die auf den Virtualisierungssystemen betriebenen virtuellen IT-Systeme kompromittiert worden sind. Dabei muss in Betracht gezogen werden, dass auf den Virtualisierungsservern selbst, aber auch auf den virtuellen IT-Systemen, Schadprogramme (Backdoors, Trojanische Pferde) installiert worden sind. Des Weiteren ist es möglich, dass über die Netzkonfiguration der Virtualisierungsserver unerwünschte Kommunikationswege geöffnet worden sind. Zudem können virtuelle IT-Systeme kopiert worden sein.

Um zuverlässig solche Schadprogramme zu entfernen, wird eine komplette Wiederherstellung der Virtualisierungskomponenten empfohlen. Hierzu können die erstellten Datensicherungen herangezogen werden, aber auch die Dokumentation der Systemkonfiguration und die Installationsanweisungen. Besitzt die eingesetzte Virtualisierungsumgebung eine Benutzerverwaltung zur Steuerung von administrativen Zugriffen, sind die Benutzerkonten, insbesondere die der Superuser, auf korrekte Gruppenmitgliedschaften zu überprüfen. Sämtliche Passwörter sollten geändert werden, um die Erfolgschancen von Folgeangriffen zu senken.

Für die virtualisierten IT-Systeme, die auf den kompromittierten Virtualisierungsservern betrieben worden sind, sollten die in den entsprechenden Notfallplänen für diese Systeme aufgeführten Maßnahmen durchgeführt werden.

Diebstahl von physischen Virtualsierungsservern

Beim Diebstahl von Virtualisierungsservern sind alle Konten zur Verwaltung der Virtualisierungsserver mit neuen Passwörtern zu versehen. Es muss damit gerechnet werden, dass auch virtuelle IT-Systeme mit dem Virtualisierungsserver gestohlen worden sind, insbesondere dann, wenn diese auf lokalen Festplatten des Virtualisierungsservers abgelegt waren. Auch wenn dies nicht der Fall ist, muss davon ausgegangen werden, dass den Dieben weite Teile der Systemkonfiguration der virtuellen IT-Systeme und der Virtualisierungsinfrastruktur im Rechenzentrum bekannt geworden sind. Daher muss geprüft werden, inwieweit Verbesserungen oder Veränderungen der Virtualisierungsinfrastruktur dazu dienen können, dass die Infrastruktur einem zukünftigen Angriff besser standhalten kann. Im Zweifelsfall sollte die komplette virtuelle Infrastruktur neu gestaltet werden.

Diebstahl von virtuellen IT-Systemen

Der Diebstahl eines virtuellen IT-Systems erfordert in der Regel keinen physischen Zugang zum Rechenzentrum. Ein Angreifer kann virtuelle IT-Systeme über Funktionen der Virtualisierungsserver z. B. kopieren. Hierzu benötigt er nur einen Netzzugang, um auf die Speicherressourcen zugreifen zu können, auf denen die virtuellen IT-Systeme abgelegt sind.

Vorbeugend sind Maßnahmen zu entwickeln, die diese Möglichkeiten erschweren. Des Weiteren muss geprüft werden, inwieweit solche Angriffe erkannt werden können. Die Notfallplanung für virtuelle IT-Systeme sollte daher Regelungen enthalten, welche die Verfahrensweise nach einem solchen Diebstahl beschreiben.

Fehlkonfigurationen

Fehlkonfigurationen von Virtualisierungsservern können zu weitreichenden negativen Folgen für den Rechenzentrumsbetrieb führen. Daher ist die Virtualisierungssoftware im Rahmen der Notfallvorsorge regelmäßig auf Fehlkonfigurationen zu überprüfen. Werden solche entdeckt, muss ihr Ausmaß bewertet werden. Hierbei ist insbesondere zu prüfen, ob virtuelle IT-Systeme durch die Fehlkonfiguration betroffen sind.

Die notwendigen Änderungen zur Behebung der Konfigurationsfehler können je nach Ausprägung direkt vorgenommen werden. Es muss allerdings beachtet werden, dass virtuelle IT-Systeme möglicherweise während solcher Änderungen beeinträchtigt werden können. Daher kann es notwendig werden, die virtuellen IT-Systeme vor Konfigurationsänderungen an den Virtualisierungssystemen herunterzufahren.

Ausfälle durch höhere Gewalt

Durch Gefährdungen aufgrund von höherer Gewalt, z. B. Erdbeben, Überschwemmung, Feuer, Sturmschäden, Kabelbeschädigungen etc., kann die Verfügbarkeit der Virtualisierungsserver negativ beeinflusst werden. Hier sind angemessene Maßnahmen zur Erhöhung der Verfügbarkeit zu prüfen, wie beispielsweise redundante Kommunikationsverbindungen der IT-Systeme.

[Quelle: BSI B 3.40Y]

A.2.3 Mehrfaktorauthentifizierung

> *Generell ist bei der Anmeldung an Diensten und Systemen – insbesondere, wenn diese online erreichbar sind – die Nutzung von mehreren Faktoren zur Erhöhung der Sicherheit gegenüber einer einfachen, auf Benutzername und Passwort basierenden Anmeldung zu empfehlen.*

Um ein angemessenes Schutzniveau („substanziell“ oder „hoch“ nach der Durchführungsverordnung (EU) 2015/1502 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der eIDAS-Verordnung) zu erreichen, ist die Nutzung von mindestens zwei unabhängigen Faktoren unterschiedlicher Kategorien zur Authentifizierung vorgesehen und in einigen Bereichen (z.B. Online-Banking und Zahlungsdienste, vgl. Delegierte Verordnung (EU) 2018/389 zur Ergänzung der PSD2-Richtlinie durch

technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation) auch gesetzlich verpflichtend umzusetzen. Im österreichischen E-Government wird die Mehrfaktorauthentifizierung durch Bürgerkarte/Handy-Signatur bzw. ID Austria umgesetzt.

A.2.3.1 Kategorien von Authentifizierungsfaktoren

Ein Authentifizierungsfaktor ist ein Element, das nachweislich mit einer Person verknüpft ist und (mindestens) einer der folgenden Kategorien angehört:

- **„besitzabhängig“:** Ein Authentifizierungsfaktor, dessen Besitz die Nutzerin bzw. der Nutzer nachweisen muss (z.B. Besitz eines Smartphones oder eines Token)
- **„kenntnisabhängig“:** Ein Authentifizierungsfaktor dessen Kenntnis die Nutzerin bzw. der Nutzer nachweisen muss (z.B. Kenntnis eins Passwortes oder einer PIN)
- **„inhärent“:** Ein Authentifizierungsfaktor, der auf ein körperliches Merkmal einer natürlichen Person abstellt und bei dem die Nutzerin bzw. der Nutzer nachweisen muss, dass er dieses körperliche Merkmal hat (z.B. Fingerabdruck oder Gesichtszüge)

A.2.3.2 Dynamische Authentifizierung

Ein wesentliches Merkmal der Sicherheit von Mehrfaktorauthentifizierungsverfahren ist, dass die Authentifizierung dynamisch erfolgt. Darunter versteht man einen elektronischen Prozess, der unter Einsatz kryptografischer oder anderer Methoden auf Abruf einen elektronischen Nachweis dafür erzeugt, dass die Benutzerin bzw. der Benutzer die Identifizierungsdaten unter ihrer bzw. seiner Kontrolle hat oder besitzt. Dieser elektronische Nachweis ändert sich dabei mit jedem Authentifizierungsvorgang zwischen dem/der Benutzer/in und dem System, das die Identität überprüft. Dadurch wird vermieden, dass eine Angreiferin oder ein Angreifer sich mit im Zuge eines Authentifizierungsvorgangs abgefangenen Daten erneut anmelden kann.

A.2.3.3 Funktionsweise

Mittlerweile werden von vielen Online-Dienstleistern Verfahren zur Mehrfaktorauthentifizierung angeboten, in den meisten Fällen handelt es sich dabei um eine Zwei-Faktor-Authentifizierung (2FA). Einige Anbieter ergänzen das zuvor eingegebene Passwort um einen zusätzlichen Faktor, andere ersetzen das vorherige – auf Benutzername und Passwort basierende Login – komplett durch eine direkte Kombination zweier Faktoren. In den meisten Fällen beginnt der

Authentifizierungsvorgang mit der gewöhnlichen Eingabe eines (gut gewählten) Passworts. Das System, in das sich die Nutzerin bzw. der Nutzer einloggen möchte, verlangt dann eine weitere Bestätigung. Dabei greifen viele übliche Zwei-Faktor-Systeme auf externe Systeme zurück, um diese zweistufige Überprüfung der Nutzerin bzw. des Nutzers durchzuführen. Bspw. kann der Anbieter einen Bestätigungscode an ein registriertes Gerät der Nutzerin bzw. des Nutzers senden (z.B. SMS oder Push-Nachricht an ein Smartphone). Der zweite Faktor kann allerdings auch ein Fingerabdruck auf einem entsprechenden Sensor oder die Verwendung eines Hardware-Tokens (USB-Token oder Smartcard) sein. Erst wenn der Besitz der Hardware oder das biometrische Merkmal nachgewiesen wird (durch Eingabe des übermittelten Codes, durch Aktivierung des Token z.B. durch Eingabe einer PIN, durch Präsentation des biometrischen Merkmals) kann der Authentifizierungsvorgang erfolgreich abgeschlossen und der betreffende Dienst oder das betreffende Gerät benutzt werden.

A.2.3.4 Gängige Systeme zur Mehrfaktorauthentifizierung

Im Wesentlichen lassen sich die von den meisten Anbietern verwendeten Systeme in drei Gruppen kategorisieren:

- **TAN/OTP Systeme:** Diese verwenden zusätzlich zum Passwort ein Einmalkennwort (TAN: Transaktionsnummer oder OTP: One-Time-Password). Die TAN bzw. das OTP wird an ein registriertes Gerät übermittelt (per SMS oder Push-Nachricht) oder von einem registrierten Gerät erzeugt (TAN/OTP Generatoren bzw. Authenticator Apps). Die Einmalkennwörter werden dabei – meist unter Verwendung von standardisierten Verfahren zeit- (TOTP - Time-based One-time Password Algorithmus, RFC 6238), ereignis- (HOTP - HMAC-based One-time Password Algorithmus, RFC 4226) oder Challenge-Response- (OCRA - OATH Challenge-Response Algorithmus, RFC 6287) basierend stets neu generiert. In der Vergangenheit wurden TANs – z.B. zur Verwendung im Online-Banking – auch als Papierlisten bereitgestellt, diese Verfahren wird aber aus Sicherheitsgründen nicht mehr eingesetzt.
  Die verschiedenen Verfahren basieren im Kern auf einer kryptografischen Hashfunktion, mit deren Hilfe aus einem geheimen Schlüssel und einem Zeit/Ereignis/Challenge-Wert ein Einmalcode generiert wird. Wesentlich für die Sicherheit des Verfahrens ist daher die Speicherung des geheimen Schlüssels. Auf Hardware-Token erfolgt diese zumeist in einem Sicherheitschip, bei Smartphone-Apps besteht eine Abhängigkeit von den Sicherheitsfunktionen des verwendeten Smartphone-Modells. Authenticator-Apps auf Smartphones bieten dafür zumeist die Möglichkeit, den Zugriff auf die App mittels biometrischer Funktionen (Fingerprint, Face-ID) oder PIN zusätzlich abzusichern. Eine weitere Erhöhung der Sicherheit bezüglich Transaktionen wird geboten, wenn Transaktionsdaten (z.B. Empfänger-IBAN, Betrag beim Online-Banking) in die Berechnung des Einmalcodes eingehen. Wird der Einmalcode per SMS oder Push-Nachricht übertragen, sollten die wesentlichen Transaktionsdaten in der

Nachricht mitgeschickt werden. Es ist davon abzuraten für den Empfang der Einmalcodes dasselbe Gerät zu verwenden, wie für das Login bzw. die Nutzung des Dienstes, da hier keine ausreichende Trennung zwischen den beiden Faktoren besteht.

- **Kryptografische Token:** Diese Token speichern einen geheimen kryptografischen Schlüssel. Im Zuge des Authentifizierungsvorgangs wird eine Anforderung an das Token gesendet, die nur mit Hilfe des geheimen Schlüssels korrekt beantwortet werden kann (ähnlich zum Challenge-Response Verfahren für OTPs). Der geheime Schlüssel kann auch in Software gespeichert werden, wesentlich sicherer ist aber die Speicherung in Hardware, z.B. auf einer Smartcard oder einem USB-/NFC-Token. Als Industriestandard für USB-/NFC-Token hat sich U2F (Universal Second Factor) der FIDO (Fast IDentity Online)-Allianz etabliert. Wenn der geheime Schlüssel in einem zertifizierten Sicherheitschip gespeichert ist, kann hier von einem hohen Sicherheitsniveau ausgegangen werden.
- **Biometrische Verfahren:** Bei System, die biometrische Verfahren nutzen, wird das Vorhandensein eines zuvor erfassten einzigartigen körperlichen Merkmals (Fingerabdruck, Gesicht, Retina etc.) überprüft. Ein wesentlicher Unterschied zu den beiden oben genannten Verfahren, die auf geheimen Schlüsseln beruhen, ist, dass biometrische Merkmale nicht „geheim“ sind. Es ist daher wichtig, dass für die Überprüfung geeignete Systeme eingesetzt werden, die eine Lebenderkennung ermöglichen, sodass das System nicht z.B. mit einem Foto oder einem kopierten Fingerabdruck getäuscht werden kann. Bei der Nutzung von Biometrie im Zhg. mit Mehrfaktorauthentifizierung ist die Sicherheit somit sehr stark von der Qualität der eingesetzten Sensoren abhängig.

A.2.3.5 Empfehlungen

Im Folgenden werden einige Empfehlungen gegeben, die speziell beim Einsatz von Mehrfaktorauthentifizierung beachtet werden sollen:

- Wenn der Faktor „kenntnisabhängig“ in Kombination mit „besitzabhängig“ verwendet wird, müssen beide Sicherungsfaktoren miteinander verknüpft sein, zum Beispiel die Benutzung einer PIN zur Freischaltung einer Smartcard.
- Eine Angreiferin bzw. ein Angreifer soll das Fehlschlagen eines Authentifizierungsversuchs nicht einem einzelnen Faktor zuordnen können. Beispielsweise soll bei Verwendung eines Anmeldeverfahrens mit Passwort und OTP-Generator nicht direkt nach Eingabe eines falschen Passwortes angezeigt werden, dass das Passwort falsch war, sondern immer die Eingabe beider Faktoren gefordert werden und dann der gesamte Anmeldeversuch als fehlgeschlagen angezeigt werden.
- Die Faktoren sollen ausreichend voneinander getrennt sein. D.h. es dürfen nicht mehrere Faktoren durch einen einzigen Angriff (z.B. durch Schadsoftware) auf die Nutzerumgebung kompromittierbar sein.

- Wenn die Faktoren nicht von der Nutzerin bzw. vom Nutzer selbst generiert werden, soll die Ausgabe der einzelnen Faktoren so erfolgen, dass diese auf verschiedenen Übermittlungswegen ausgegeben werden. Dies kann auch geeignet umgesetzt werden, indem die Faktoren zeitlich getrennt auf gleichem Wege übermittelt werden, sofern sichergestellt ist, dass ein Faktor die Inhaberin bzw. den Inhaber erreicht hat, bevor der nächste übermittelt wird.
- Bei Verwendung von Software-Token sollen die privaten kryptografischen Schlüssel nicht außerhalb des Tokens vorliegen. Das Schlüsselmaterial muss dazu auf dem Computersystem mindestens durch Softwaremechanismen vor Kopieren oder Export geschützt sein. Weitere Schutzmechanismen wie z. B. Windows Zertifikatsspeicher oder macOS Schlüsselbund sollen verwendet werden. Das Computersystem, auf dem der Token gespeichert ist, sollte ausschließlich durch die Token-Inhaberin bzw. den Token-Inhaber genutzt werden. Es dürfen nur vorab definierte und eingeschränkte Nutzergruppen Zugriff auf das Computersystem haben. Das Speichern auf Computersystemen, die möglicherweise auch für Unbekannte zugänglich sind (z.B. einer öffentlichen Cloud) ist nicht zulässig.
- Sofern Schlüssel außerhalb des Tokens erzeugt werden, muss dies in einer sicheren Umgebung erfolgen und die außerhalb des Tokens vorliegenden privaten Schlüssel müssen vor Auslieferung des Tokens gelöscht werden
- Bei TAN/OTP Verfahren sollen wesentliche Vorgangsdaten (z.B. Empfänger-IBAN und Betrag bei Online-Überweisungen) in die Erzeugung des Einmalcodes eingehen und der Nutzerin bzw. dem Nutzer unabhängig von der primären Verbindung angezeigt werden.
- Die TAN/OTP-Generatoren müssen individuell sein, d.h. es soll nicht möglich sein, den TAN/OTP-Generator einer anderen Inhaberin bzw. eines anderen Inhabers für die Anmeldung zu verwenden.
- Die Registrierung von Geräten (SIM-Karte/Telefonnummer, Smartphone) soll mit einem Verfahren erfolgen, dass mindestens dem Sicherheitsniveau „substanziell“ entspricht.
- Für die Rücknahme einer Sperrung eines Authentifizierungsmittels – sofern dies vom System unterstützt wird – muss eine Identifizierung der Inhaberin bzw. des Inhabers dieses Authentisierungsmittels mindestens auf dem Vertrauensniveau des Authentifizierungssystems erfolgen.
- Bei der Reaktivierung eines Authentifizierungsmittels muss sichergestellt sein, dass die Sicherheit des Authentifizierungsmittel nicht kompromittiert wurde.

[basierend auf BSI TR-03107-1]

A.3 Cloud Computing

Dieser Anhang stellt Grundlageninformationen für strategische Entscheidungen zum Thema Cloud Computing bereit bzw. erörtert, wie notwendige Entscheidungsgrundlagen erarbeitet werden können und welche Aspekte dabei beachtet werden müssen. Der Anhang definiert dazu relevante Begriffe und diskutiert ausgewählte rechtliche, organisatorische, wirtschaftliche und technische Aspekte des Themenkomplexes Cloud Computing. Zudem werden Auswirkungen, Chancen und Risiken sowie potenzielle Anwendungen von Cloud Computing zusammenfassend erörtert. Damit gibt dieser Anhang einen ersten Einblick zum Thema Cloud Computing und stellt einen Einstiegspunkt in diese komplexe Materie dar.

Für weiterführende und tiefergehende Informationen zum Thema Cloud Computing seien interessierte Leserinnen und Leser an den von der A-SIT Plus GmbH herausgegebenen Cloud Computing Kompass [CLD-KOM] verwiesen. Dieser wurde im Rahmen des KIRAS-Projekts SECCAT von der A-SIT Plus GmbH in Zusammenarbeit mit IDC Central Europe GmbH, EuroCloud.Austria, REPUCO Unternehmensberatung GmbH und dem Bundesministerium für Finanzen erstellt und bietet einen umfassenderen Einstieg in das Thema Cloud Computing.

Weiters bietet das deutsche BSI mit dem Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) eine Auflistung an Mindestanforderungen für sicheres Cloud-Computing als Hilfestellung sowohl für professionelle Cloud-Anbieter als auch deren Kunden. Eine spezialisiertere Variante wurde mit dem Kriterienkatalog AIC4 (Artificial Intelligence Cloud Service Compliance Criteria Catalogue) geschaffen, der Mindestanforderungen an die sichere Verwendung von Methoden des maschinellen Lernens in Cloud-Diensten spezifiziert.

Einleitung

Cloud Computing ist eine Form der flexibel am Ressourcenbedarf orientierten Nutzung von IT-Leistungen und der Unabhängigkeit von konkreten Plattformen, da Verarbeitungen entweder in der Cloud oder in einer sehr standardisierten Form erfolgen. Benötigte Ressourcen werden in Echtzeit als Service über das Internet bzw. Intranet bereitgestellt und meist nach Nutzung abgerechnet. Viele der Services erscheinen den Nutzern kostenfrei zu sein. Tatsächlich handelt es sich jedoch um eine Umschichtung des Kostenmodells, wodurch sich unter anderem die Notwendigkeit eines genaueren Blicks auf Datenschutzbestimmungen ergibt.

Nutzer von Cloud-Services müssen IT-Ressourcen nicht selbst anschaffen und betreiben, sondern nutzen die nötigen Kapazitäten für Daten, Rechenleistung und Anwendungen bei Anbietern als „Services aus dem Netz“. Damit ermöglicht Cloud Computing den Nutzern einen bedarfsgerechten und vor allem dynamischen und einfach zu skalierenden Einsatz von Mitteln und eine Umverteilung von Investitions- zu Betriebsaufwänden. Beides kann für hohe Flexibilität sorgen. Cloud Computing ist keine grundsätzlich neue Technologie, sondern kombiniert vorhandene Technologien und Verfahren für eine standardisierte Bereitstellung von Diensten (Services) und ist daher eine Weiterentwicklung des Outsourcing-Modells. Durch die Anforderungen des Cloud Computing wurden aber Technologien stark weiterentwickelt und auf eine neue Ebene im Bereich Skalierung, Flexibilität, Nutzungsgrad und geteilte Nutzung gebracht. Dadurch ergeben sich durch Cloud Computing neue Chancen, aber auch Risiken.

Dieser Anhang des österreichischen Sicherheitshandbuchs beruht unter anderem auf einem von der Plattform Digitales Österreich erstellten Positionspapier [IKT-CLOUD] und soll Grundlageninformationen für nötige strategische Entscheidungen bereitstellen bzw. dabei unterstützen, diese Entscheidungsgrundlagen selbstständig zu erarbeiten. Dazu definiert der Anhang relevante Begriffe und diskutiert themenbezogene rechtliche, organisatorische, wirtschaftliche und technische Aspekte.

A.3.1 Begriffsdefinitionen

Cloud Computing ist ein Begriff, der seit vielen Jahren die IT-Landschaft prägt und mittlerweile sowohl im professionellen als auch im privaten Umfeld nicht mehr wegzudenken ist. Vor allem im professionellen Umfeld ist einer der Schlüsselaspekte hinter dem breiten Interesse an Cloud Computing die mögliche wirtschaftliche Effizienzsteigerung im Vergleich zu traditionellen Methoden der Bereitstellung von IT-Ressourcen. Bei privaten Benutzerinnen und Benutzern wird Cloud Computing vor allem auch mit einer erhöhten Benutzerfreundlichkeit (durch Einfachheit in der Verwendung) in Verbindung gebracht, die sich vor allem bei der Nutzung mobiler Endnutzergeräte bemerkbar macht. Zur oft genannten Kosteneffizienz von Cloud Computing ist anzumerken, dass diese nach wie vor auf strategischen Preisbildungen seitens der Anbieter beruhen und damit die Stabilität der Preise vom Willen der Anbieter abhängen.

Der Begriff Cloud Computing bezeichnet ganz allgemein das Anbieten bzw. Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden. Charakteristisch ist für Cloud Computing außerdem, dass Ressourcen oder Dienste nicht unbedingt dediziert einem Kunden zugeordnet, sondern auch dynamisch je nach Bedarf – und Vertragsmodell – zur Verfügung gestellt werden.

Grob zusammengefasst beschreibt Cloud Computing damit eine bedarfsgerechte und flexible Bereitstellung von IT-Ressourcen, wobei ausschließlich deren tatsächliche Nutzung abgerechnet wird. In Bezug auf involvierte Stakeholder haben sich im Kontext Cloud Computing folgende Begriffe etabliert:

- **Cloud-Service:**
  Das über eine Cloud-Infrastruktur bereitgestellte Service. Dabei kann es sich um eine konkrete Anwendung (Software), eine Plattform oder auch um IT-Infrastruktur (z.B. einen virtuellen Server) handeln.
- **Cloud-Service-Provider (CSP):**
  Anbieter des Cloud-Service und damit Betreiber der für das Cloud-Service benötigten IT-Infrastruktur.
- **Kunde:**
  Der gegenüber dem Cloud-Service-Provider (CSP) auftretende Auftraggeber.
- **Anwender/Benutzer/Nutzer:**
  Die das Cloud-Service nutzende Entität. Diese kann der Kunde selbst sein oder zum Beispiel im Fall, dass ein Unternehmen als Kunde/Auftraggeber fungiert, auch ein Mitarbeiter des Unternehmens.

Der Begriff Cloud Computing ist relativ allgemein und umfasst ein sehr breites Spektrum von Diensten zur Bereitstellung von IT-Ressourcen und Services. Eine differenzierte Betrachtung des Themas macht daher eine Kategorisierung und Unterteilung der unter dem Begriff Cloud Computing subsummierten Ansätze und Lösungen notwendig. Das National Institute of Standards and Technology (NIST) kategorisiert Cloud Computing-Dienste anhand von Charakteristiken, Servicemodellen sowie Einsatzvarianten. Diese Kategorien werden in den folgenden Unterabschnitten beschrieben.

A.3.1.1 Charakteristiken von Cloud Computing

Cloud Computing zeichnet sich durch die im Folgenden gelisteten Charakteristiken aus. Es werden hier bewusst die englischen Begriffe verwendet, da diese im Kontext Cloud Computing etabliert sind. Wo sinnvoll, sind die entsprechenden deutschen Begriffe daneben in Klammern angeführt.

- **On-Demand Self-Service / Self-provisioning of resources**
  (Ressourcenmanagement durch Nutzer/Kunden)
  Ein Kunde (s.o.) kann selbstständig und vollautomatisch Rechenressourcen wie Rechenleistung oder Netzwerkspeicher, Anwendungen, Upgrades etc. abrufen und buchen, ohne dass hierzu eine Interaktion mit dem CSP nötig ist.
- **Broad Network Access**

Sämtliche Ressourcen sind breitbandig über das Internet oder Intranet angebunden. Der Zugriff erfolgt über Standardmechanismen, die eine Nutzung von Cloud-basierten Diensten mittels herkömmlicher Server oder auch Endgeräte wie PCs, Laptops, Tablets oder Smartphones ermöglichen.

- **Resource Pooling**
  Die Rechenressourcen des CSP werden an einer Stelle gebündelt und mehreren Nutzern zur Verfügung gestellt.
- **Massive Scalability** (Skalierbarkeit)
  Je nach Anforderungen können Ressourcen im entsprechenden Umfang dem Kunden zur Verfügung gestellt werden.
- **Rapid Elasticity** (Elastizität)
  Ressourcen können in Echtzeit schnell und teilweise automatisiert auf die veränderten Bedürfnisse des Nutzers angepasst werden. Aus der Sicht der Nutzer stehen damit praktisch unbeschränkt Ressourcen zur Verfügung, die jederzeit und in jedem Umfang gekauft bzw. genutzt werden können. Dank der dynamischen Verteilung von Ressourcen und Diensten können so bspw. Lastspitzen gut ausgeglichen werden.
- **Measured Service / Pay as you go** (verbrauchsorientiertes Bezahlmodell)
  Cloud Computing Systeme kontrollieren und optimieren die Zuteilung von Ressourcen vollautomatisiert. Der Ressourcenverbrauch wird kontinuierlich gemessen, kontrolliert und berichtet, um Transparenz für den Provider und den Kunden herzustellen. Nur die genutzten Dienste und Ressourcen werden abgerechnet - Nutzer zahlen in der Regel nur für tatsächlich abgerufenen Ressourcen und Dienste (je nach Vertragsmodell).
- **Multitenancy** (Mehrmandantenfähigkeit)
  Ressourcen und Dienste werden zwischen allen Kunden/Nutzern dynamisch aufgeteilt.
- **Push Notification**
  Nachrichten werden unaufgefordert auf Geräteebene zum Anwender gesendet, um Aktivitäten des Benutzers auszulösen. Diese Kommunikation ersetzt zunehmend die Aufforderung zur Aktion per E-Mail oder andere klassische Verbindungen.

A.3.1.2 Servicemodelle des Cloud Computing

Im Zusammenhang mit Cloud Computing existiert eine Klassifizierung von Cloud-Services in die drei unten angeführten grundlegenden Modelle:

- **Infrastructure as a Service (IaaS):**
  Bei IaaS werden grundlegende Infrastrukturleistungen zur Verfügung gestellt (z.B. Rechenleistung, Speicherplatz), auf deren Basis der Nutzer individuelle Software wie Betriebssysteme oder Anwendungsprogramme betreiben kann. Der Nutzer ist nicht für das Management oder die Wartung der

Infrastruktur zuständig, hat aber dennoch die Kontrolle über Betriebssysteme, Speicherverwaltung und Anwendungen. Auf die Konfiguration bestimmter Infrastrukturkomponenten, wie bspw. Host-Firewalls, hat er evtl. eine beschränkte Einflussmöglichkeit.

- **Platform as a Service (PaaS):**
  Nutzer können auf Basis einer Cloud-Plattform Anwendungen entwickeln oder bereitstellen. Dazu werden entsprechende Frameworks und Entwicklungswerkzeuge zur Verfügung gestellt. Dabei hat der Nutzer die Kontrolle über die Anwendungen und individuelle Konfigurationsparameter der Bereitstellungsumgebung.
- **Software as a Service (SaaS):**
  Bei SaaS wird dem Nutzer eine Anwendung als Dienst zur Verfügung gestellt. Die Änderung nutzerspezifischer Konfigurationseinstellungen ist evtl. nur eingeschränkt durch den Nutzer möglich.

Der Begriff „as a Service“ ist mittlerweile breit etabliert und wird im Zusammenhang mit einer Vielzahl weiterer Cloud-Service-Angebote genutzt. Dazu zählen unter anderem:

- Communications as a Service
- Data Storage as a Service
- Desktop as a Service
- Federation as a Service
- Identity as a Service
- Network as a Service
- Security as a Service

A.3.1.3 Ausprägungen von Cloud Computing

In der Praxis sind drei grundsätzliche Ausprägungen (Betriebsmodelle) für Cloud Computing zu unterscheiden. Diese (und etwaige Untervarianten) sind im Folgenden ausgeführt.

- **Public Cloud:** Die vom CSP betriebene Cloud-Infrastruktur ist öffentlich über Internettechnologien zugänglich. In der Regel wird diese Ausprägung von einer sehr großen Nutzeranzahl in Anspruch genommen, wodurch sich entsprechende Skaleneffekte erzielen lassen. Durch die hohe Anzahl der Nutzer ist eine Individualisierung der Dienste und eine maßgeschneiderte Anpassung hier am wenigsten möglich.

    - **Virtual Private Cloud:** Eine Virtual Private Cloud ist eine spezifische Ausprägung einer Public Cloud, bei der mittels geeigneter Sicherheitsvorkehrungen dem Kunden eine abgekapselte IT-Infrastruktur zur Verfügung gestellt wird, die unter Verwendung der VPN (Virtual Private Network)-Technologie abgesichert mit dem Netzwerk des Kunden verbunden ist.
- **Private Cloud:** Die Cloud-Infrastruktur wird für einen einzelnen Auftraggeber bzw. für eine vorgegebene Gruppe betrieben, die ausschließlichen Zugriff auf die Cloud hat. Sie kann die Infrastruktur selbst oder durch Dritte betreiben lassen. Zwar werden so Skaleneffekte und Kosteneinsparungen reduziert, jedoch sind dafür stärkere Individualisierungen der Dienste (d.h. Anpassung auf die Erfordernisse der Kunden) möglich. Aus Sicht des Auftraggebers nimmt die Kontrolle über die Cloud zu.
    - **Community Cloud:** Im Rahmen einer Community Cloud wird die Cloud-Infrastruktur gemeinsam von mehreren Organisationen genutzt, die ähnliche Interessen bzw. Ziele verfolgen. Das Management der Infrastruktur erfolgt durch die Organisationen selbst oder extern durch einen Dritten.
- **Hybrid Cloud:** Die hybride Variante einer Cloud-Infrastruktur ist eine Mischung zweier oder mehrerer Varianten. Dabei bleiben die unterschiedlichen Clouds eigenständige Einheiten, die jedoch mit standardisierter oder proprietärer Technologie miteinander verbunden werden. So wird die Daten- bzw. Anwendungsportabilität sichergestellt. Mittels einer Hybrid Cloud können die Vorteile mehrerer Varianten kombiniert und Kostenvorteile von Public Clouds mit Sicherheitsvorteilen von Private Clouds kombiniert werden. Allerdings ist hierbei auch eine strikte und somit oftmals kostspielige Trennung der Daten notwendig.

A.3.2 Rechtliche Aspekte

Aus rechtlicher Sicht betrifft Cloud Computing mehrere Gebiete [CCDS]. Dieser Abschnitt gibt einen Überblick über potenzielle relevante rechtliche Aspekte im Kontext Cloud Computing. Der gegebene Überblick bleibt jedoch bewusst oberflächlich und erhebt keinen Anspruch auf Vollständigkeit.

A.3.2.1 Grundsätzliches

Aus rechtlicher Sicht sind im Kontext Cloud Computing unter anderem folgende Gebiete von besonderer Bedeutung, auf die in den folgenden Unterabschnitten näher eingegangen wird:

- Datenschutzrecht
- IT-Vertragsrecht
- Vergaberecht
- Strafprozessrecht

Wie bei allen Outsourcing-Modellen ist auch bei Cloud Computing bewusst auf Unternehmensveräußerung, Konkurs und Liquidation sowie Zugriff auf die 'eigenen Daten' im Detail rechtlich einzugehen.

A.3.2.2 Datenschutz

Gerade im Kontext von Cloud Computing müssen rechtliche Vorgaben in Bezug auf den Datenschutz berücksichtigt werden. Es gelten auch hier die Vorgaben der Datenschutzgrundverordnung (DSGVO) bzw. der entsprechenden nationalen Gesetzgebungen wie dem österreichischen Datenschutzgesetz (DSG).

Datenschutzthemen müssen dann berücksichtigt werden, wenn über das angebotene und konsumierte Cloud-Service personenbezogene Daten verarbeitet werden. Werden keine personenbezogenen Daten verwendet, ist keine weitere datenschutzrechtliche Prüfung erforderlich.

Bei einer Verarbeitung von personenbezogenen Daten sind bei der Wahl des Cloud-Service-Providers (CSP), welcher als Auftragsverarbeiter im Sinne des Art. 4 Z 8 DSGVO zu beurteilen ist, nachstehende Fragen zum Datenschutz zu prüfen. Nur wenn all diese Fragen mit „Ja“ beantwortet werden können, ist eine Einhaltung der datenschutzrechtlichen Vorgaben gegeben. Relevante Fragestellungen sind in verschiedene Kategorien, repräsentiert durch die folgenden Unterabschnitte, unterteilt.

Verarbeitungs- bzw. Speicherort von Daten (Storage)

Bestimmte Datenschutzbestimmungen verbieten den Transfer von Daten im Klartext in andere oder bestimmte Länder, oder es ist die explizite Zustimmung durch jene Person, auf die sich die Daten beziehen, erforderlich. Eine dynamische Umverteilung im Laufe der Zeit ist mit zu beachten. Bestehende Regelungen, wonach Daten ausschließlich im Inland gespeichert werden dürfen (z.B. im Zusammenhang mit der umfassenden Landesverteidigung), schließen CSP außerhalb Österreichs aus. In Bezug auf den Verarbeitungs- und Speicherort von Daten ergeben sich damit folgende relevante Fragestellungen:

- Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, für die ein Angemessenheitsbeschluss der Kommission vorliegt, verarbeitet?
- Wenn nein, liegen sonstige geeignete Garantien vor (Standarddatenschutzklauseln, von der zuständigen Aufsichtsbehörde genehmigte verbindliche, interne Datenschutzvorschriften, genehmigte Verhaltensregeln oder genehmigter Zertifizierungsmechanismus)?

- Wenn nein, liegt mindestens einer der folgenden Gründe vor: eine ausdrückliche Einwilligung des Betroffenen, die Übermittlung ist zur Erfüllung eines Vertrages auf Antrag der betroffenen Person erforderlich, zur Erfüllung eines im Interesse der betroffenen Person liegenden Vertrags, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz lebenswichtige Interessen der betroffenen oder einer anderen Person oder aus wichtigen Gründen des öffentlichen Interesses?

Grundlage und Art der Verarbeitung

- Bietet der Auftragsverarbeiter hinreichende Garantien, dass ausreichende organisatorische und technische Maßnahmen gesetzt sind sowie Fachwissen, Kompetenz, Zuverlässigkeit und dergleichen bestehen, um den Anforderungen der DSGVO und des DSG gerecht zu werden?
- Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten?
- Wurde vom Auftragsverarbeiter ein Datenschutzbeauftragter bestellt?
- Nimmt der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter in Anspruch, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen?
- Erfolgt die Verarbeitung auf Grundlage eines Vertrages oder eines anderen in der DSGVO oder im DSG genannten Rechtsinstruments der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind?

Datensicherheitsmaßnahmen

Zentral für die Einhaltung relevanter Datenschutzanforderungen ist die Implementierung geeigneter Datensicherheitsmaßnahmen. In diesem Zusammenhang ergeben sich folgende relevante Fragestellungen:

- Stellt der Auftragsverarbeiter die Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO sicher?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zur Pseudonymisierung oder Verschlüsselung personenbezogener Daten?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen gegen den Verlust oder unbefugtem Zugriff auf die Daten?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zur Protokollierung der Zugriffe?
- Hält der Auftragsverarbeiter die Grundsätze des Datenschutzes durch Technik (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default) durch entsprechende Maßnahmen ein?
- Ist beim Auftragsverarbeiter ein Prozess implementiert, der die regelmäßige und anlassbezogene Evaluierung der Datensicherheitsmaßnahmen sicherstellt?

Betroffenenrechte (Auskunfts-, Berichtigungs-, Löschungs-, Widerspruchs- und Einschränkungsrecht, Datenübertragbarkeit) gemäß Art. 12 – 23 DSGVO

Die Person, auf die sich die verarbeiteten Daten beziehen (d.h. der/die Betroffene im Sinne des DSG bzw. der DSGVO), kann sowohl Auskunft über verarbeitete Daten, als auch Korrektur, das Löschen, die Einschränkung der Verarbeitung oder die Übertragung dieser Daten verlangen. In Bezug auf Betroffenenrechte ergeben sich damit folgende relevante Fragestellungen:

- Ist sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen, die Einschränkung der Verarbeitung oder die Übertragung der Daten der Betroffenen in der Cloud gemäß den rechtlichen Vorgaben gewährleistet und durchführbar?
- Gibt es ein Regelwerk, das das Verfahren zur Wahrung der Rechte der Betroffenen im Fall von gemeinsam Verantwortlichen klar regelt?

Verbleib und Vernichtung von Daten (Retention/Destruction)

Am Ende der Haltezeit von Daten müssen diese geeignet gelöscht werden. Folgende relevante Fragestellungen stehen mit dieser Anforderung im Zusammenhang:

- Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)?
- Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten?
- Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)?
- Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Backup) erhalten bleiben?
- Gibt es ein Regelwerk, wonach die Zurückstellung (inkl. Löschung der Daten beim CSP) an den Verantwortlichen nach Beendigung des Vertragsverhältnisses erfolgt?

Datenschutzverletzungen (Privacy Breaches)

Für den Fall von Datenschutzverletzungen müssen definierte Prozess und Vorgehensweisen existieren, über die notwendige schadensminimierende Schritte geregelt sind. In diesem Zusammenhang ergibt sich folgende relevante Fragestellung:

- Ist bei Datenschutzverletzungen ein Meldeprozess bei Verantwortlichem und Auftragsverarbeiter etabliert?

A.3.2.3 Vertragsrecht

Vertragliche Regelungen mit dem CSP sollten prinzipiell immer auf den Einzelfall abgestimmt sein. Folgende Punkte können jedoch Inhalt einer vertraglichen Regelung sein:

- Zusicherung der Einhaltung der datenschutzrechtlichen Anforderungen;
- Informationsverfahren bei datenschutzrechtlichen Verletzungen;
- Gewährung eines Kontrollzugriffs durch den Verantwortlichen;
- Auftragsverarbeitervereinbarungen (abhängig von der Anzahl der Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter die in Anspruch genommen werden);
- Art der Leistung (Leihe, Miete, Werk- oder Dienstleistung);
- Haftung und Gewährleistungsansprüche;
- Service-Level-Agreement (SLA);
- Sonstige Vereinbarungen (z.B. ISO 27001, Informationssicherheitsmanagementsystem (ISMS));
- Einhaltung referenzierter Konvention (internationale Standards, BLSG-Konventionen);
- Migrierbarkeit der (Daten-)Standards im Fall des Betreiberwechsels, Unternehmensübergang oder im Insolvenzfall;

Eine gute Aufgliederung notwendiger vertraglicher Regelungen (auch) über die datenschutzrechtlichen Punkte hinaus findet sich etwa unter [LCCR], [BITK10] oder auch im Cloud Computing Kompass [CLD-KOM].

A.3.2.4 Vergaberecht

Cloud Service Provider sind meist international tätig und stellen ihre Leistungen unter Standard-AGB zur Verfügung. Es ist daher zu prüfen, ob sich diese CSP überhaupt an einem formellen Ausschreibungsverfahren beteiligen würden und sich notwendige Abweichungen von den AGB mit dem jeweiligen CSP vereinbaren lassen.

A.3.2.5 Strafprozessrecht

Es sind innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden zu beachten (z.B. Verkehrsdaten).

A.3.3 Organisatorische Aspekte

In diesem Abschnitt werden Chancen und Risiken des Cloud Computing aus der organisatorischen Perspektive dargestellt und mögliche Auswirkungen von Cloud Computing auf die IT-Organisation erläutert. Im Fokus der Betrachtung steht dabei das Modell „Public Cloud“, da sich hier die größten organisatorischen Änderungen im Vergleich zu einer klassischen IT-Infrastruktur (on-premise) ergeben. Wesentliche Teile der Überlegungen gelten jedoch auch für die Modelle „Private Cloud“ und „Community Cloud“.

A.3.3.1 Grundsätzliches

Cloud Computing kann organisatorische Vorteile durch Standardisierung bieten. Organisatorische Nachteile und Risiken inkludieren eine erschwerte Steuerung des IT-Einsatzes, strukturelle Abhängigkeit aufgrund von Lock-in-Effekten gegenüber Cloud-Anbietern sowie die Notwendigkeit der Kontrolle der Einhaltung von Governance-Regeln [DSCC10].

Cloud Computing stellt die organisatorische Steuerung der IT vor zahlreiche Herausforderungen. Einige der wichtigsten Herausforderungen sind im Folgenden gelistet und beschrieben.

- Standardisierung: Prinzipiell bietet Standardisierung in der IT neben der Kostenreduktion auch diverse organisatorische Vorteile (z.B. Vereinfachung von Prozessen, Integration externer Partner, Flexibilität und Agilität). Cloud Computing ist, sofern richtig eingesetzt, eine Möglichkeit, Standardisierung zu fördern und entsprechende Vorteile zu generieren. Falsch eingesetzt kann Cloud Computing jedoch auch zu gegenteiligen Ergebnissen führen. Bei den Standardisierungen im E-Government-Umfeld sollte darauf Rücksicht genommen werden, dass Cloud nicht prinzipiell ausgeschlossen wird. Bislang sind die Tendenzen der großen Cloud-Anbieter noch immer reichlich proprietär und damit hemmen diese die Effekte des Marktes. Lediglich bei Open-Source Ansätzen kann man von einer kontrollierbaren, herstellerunabhängigen Situation ausgehen.
- Organisatorische Aufspaltung: Cloud Computing kann zu „Silo-Lösungen“ führen, wenn die Zusammenhänge zwischen Anwendungen und Prozessen bei Entscheidungen nicht berücksichtigt werden. In solchen Situationen kann sich der Datenaustausch zwischen Anwendungen (bei „Silo-Lösungen“) als schwierig erweisen, was wiederum die Service-Qualität aus der Perspektive des Auftraggebers reduziert. In diesem Aspekt haben „Mobile First“ und „Cloud“ relativ ähnliche Effekte. Damit werden mittel und längerfristig Anwendungen und Prozesse angehalten sein, sich in kleine Schritte mit fest definierten

Schnittstellen zu teilen. So können einzelne Schritte für den Massenbetrieb in Cloud-Prozesse ausgelagert und vorerst für den Notbetrieb lokal als Backup-Variante und zum Sicherstellen der nachhaltigen Schnittstellenkompatibilität parallel gehalten werden.

- Strukturelle Abhängigkeit: Durch zu starke Bindung an einen bestimmten CSP oder einen Service können Abhängigkeiten bis hin zu Lock-in-Effekten entstehen, die einen Wechsel zu einem anderen Dienstleister oder einem internen Service erschweren. Potenzielle Abhängigkeiten und Migrationskosten sollten deshalb stets berücksichtigt werden.
- Potenzielle Steigerung des Verarbeitungsvolumens: Bei einem Einsatz von Cloud Computing werden grundsätzlich sinkende Kosten erwartet. In der Praxis kann es aber aufgrund gesteigerter Nutzung entsprechender Services zu höheren Verbrauchsmengen und damit in weiterer Folge schnell zu unerwartet steigenden Kosten kommen. Cloud-Preise sind nach wie vor strategisch durch die Anbieter definiert und ergeben sich nicht ausschließlich aus tatsächlichen Komponentenpreisen. Dieser Umstand verstärkt die Notwendigkeit, sich auf Standards von Services und offene Schnittstellen zu konzentrieren, um auch mittelfristig von den Skaleneffekten der Cloud profitieren zu können.
- Fehlender Kostenvergleich: In Organisationen sind die internen Kosten bei fehlender Kostenrechnung oft nicht exakt bekannt. Ein aussagekräftiger Vergleich der Kosten zwischen einer Cloud-Lösung und einer internen Lösung ist dann oftmals nicht oder nur schwierig möglich.
- Vereinbarungen: Oftmals ist in einer traditionell strukturierten internen IT-Abteilung wenig Erfahrung mit Dienstleistern und entsprechenden Vereinbarungen vorhanden. Gerade sorgfältig ausgearbeitete Bestimmungen in den Dienstleister- bzw. Betriebsvereinbarungen sind für einen erfolgreichen Einsatz von Cloud Computing aber von großer Bedeutung. Zu berücksichtigende Aspekte beinhalten u.a. Service Level Agreements (SLA), Verfügbarkeitsvereinbarungen, Regelungen zum Change-Management, Notfallmanagement oder auch Qualitätssicherung. Auch die Kontrolle dieser Vereinbarungen muss organisatorisch berücksichtigt werden.

Um die Risiken des Cloud Computing zu minimieren bzw. die Potenziale bestmöglich auszuschöpfen, ist eine ausführliche Voranalyse über Ziele und Anforderungen erforderlich. Idealerweise wird dabei ein Vorgehensmodell zur Einführung von Cloud Computing eingesetzt [PCEC09]. Ein Beispiel dafür ist das fünfstufige Vorgehensmodell von Reeves und Santos [BSCA10], das die folgenden Schritte umfasst:

1. Projektvorbereitung:
    - Formierung eines Kernteams zur Entwicklung einer Cloud-Strategie
    - Definition von Geschäftszielen und Darlegung der Migrationsgrundsätze
    - Entwicklung einer Migrations-Roadmap sowie Sicherstellung der Nachhaltigkeit von Schnittstellen und Gliederung in möglichst überschaubare und unabhängige Teilprozesse

2. Analyse des Geschäftsfeldes sowie der bestehenden IT-Anwendungen
    - Identifizierung der Risiken und der Einflüsse im Falle eines Ausfalls der Cloud
    - Analyse der Anforderungen und Abhängigkeiten der IT-Anwendungen
    - Kostenvergleich Cloud vs. on-premise Betrieb der IT-Anwendungen
    - Analyse der Änderung der internen organisatorischen Abläufe sowie generelle Auswirkungen auf die Organisation
    - Erarbeitung von Richtlinien zur Bestimmung des passenden Cloud-Modells (Software as a Service, Platform as a Service, Infrastructure as a Service) bzw. der Ausprägung (Private Cloud, Public Cloud oder Hybrid Cloud)
3. Auswahl des Cloud-Anbieters
    - Analyse des Leistungsvermögens sowie des Risikopotenzials der Cloud-Anbieter anhand der ermittelten Anforderungen und den vorliegenden Angeboten
    - Entscheidung nach Einsatz von geeigneten Evaluierungsverfahren
4. Vermeidung bzw. Reduzierung der Risiken durch Planung einer Exit-Strategie bzw. eines lokalen Backup-Service für wesentliche Applikationen
5. Planung des laufenden Betriebes über die Erarbeitung von Governance-Regeln (Management von unerwarteten Ausgaben, Budgetplanung, ungeplante Auswirkungen)

Von **zentraler Bedeutung** ist während der Planung des Einsatzes von Cloud Computing die **Analyse der „Cloud-Fähigkeit“** von IT-Anwendungen. Aus organisatorischer Perspektive sind (bei Cloud Computing) folgende Aspekte zu berücksichtigen [BSCA10]:

- Kontinuität: Es gilt abzuklären, welche Auswirkungen auf die Kontinuität der Geschäftstätigkeit vorherrschen und damit zu bestimmen, wann eine IT-Anwendung zu geschäftskritisch ist, um in die Cloud ausgelagert zu werden und wie hoch der Schwellenwert für Ausfallszeiten liegt bzw. wann eine lokale Backup-Situation vorzusehen ist.
- Informationssicherheit: Es ist festzustellen, welche Daten eine IT-Anwendung aufgrund der besonderen Sensitivität für (Public-)Cloud Computing disqualifizieren bzw. welche kryptographischen Funktionen dieses Problem vermeiden können.
- Risikotoleranz: Es ist zu klären, welche Risiken für eine Organisation (z.B. aufgrund von Service-Ausfällen) tragbar sind und ob ein Schwellenwert besteht, der durch ein SLA nicht garantiert werden kann.
- Interdependenz von IT-Anwendungen: Es gilt abzuklären, welche Abhängigkeiten einer IT-Anwendung bestehen bzw. ob Abhängigkeiten bestehen, die eine Auslagerung unmöglich machen.

- Migrationsaufwand: Der maximal tolerierbare Aufwand für die Migration einer IT-Komponente (Infrastruktur, Plattform, Software) in die Cloud ist festzustellen und als Verhältnis den erwartbaren Einsparungen gegenüber zu stellen (Kosten-Nutzen-Analyse).

Generell gilt es, die Berücksichtigung der Cloud-Fähigkeit von neuen Applikationen bereits in der Architekturphase und Vergabephase zu prüfen und bei positiver Einschätzung weitere Schritte zu setzen bzw. eine entsprechende Analyse durchzuführen (z.B. durch das skizzierte fünfstufige Vorgehensmodell).

A.3.4 Wirtschaftliche Aspekte

In vielen Fällen ist eine Verwendung von Cloud Computing von wirtschaftlichen Überlegungen getrieben, etwa wenn aus einer Verlagerung von Services in die Cloud Kostenersparnisse erhofft werden. Relevante wirtschaftliche Aspekte, die sich im Zusammenhang einer Verwendung von Cloud Computing ergeben, sind in diesem Abschnitt diskutiert.

A.3.4.1 Grundsätzliches

Die Cloud-Service-Provider (CSP) realisieren Kostenvorteile vor allem durch das Standardisieren von Services, das Bündeln von IT-Ressourcen und die Automatisierung von Abläufen. Die Kalkulationen und Wirtschafts- bzw. Geschäftsmodelle sind allerdings für Kunden großer CSP kaum nachzuvollziehen. Auf Anbieterseite ermöglicht Cloud-Computing weitreichende Skaleneffekte. So sinken mit zunehmender Auslastung auf Anbieterseite die (Betriebs-)Kosten (Strom – GreenIT/CO2 Reduktion, Sicherheit, etc.) pro Server. Gleichzeitig können die Overhead-Kosten auf Anbieterseite auf eine größere Zahl von Nutzern aufgeteilt werden. Der Kunde profitiert zudem durch ein höheres Maß an Flexibilität und budgetärem Planungsspielraum, da er die Ressourcen des CSP exakt seinem Bedarf entsprechend – also auch kurzfristig – in Anspruch nehmen kann. Investitionskosten zum Abdecken von Auslastungsspitzen können entfallen. Das Risiko, insbesondere das Sicherheitsrisiko, wird zwar geringer aber dennoch zentralisiert, wodurch auch der Nutzen eines erfolgreichen Angriffes steigt. Dies macht Cloud-Services zu einem attraktiven Ziel für Angreifer.

Relevante wirtschaftliche Aspekte des Cloud Computing können unter diesen Gesichtspunkten wie folgt zusammengefasst werden:

- Standardisierte IT-Infrastrukturen und IT-Dienste sind unter den Rahmenbedingungen einer Cloud-Architektur und eines Cloud-Geschäftsmodells wirtschaftlicher zu beziehen bzw. zu erbringen.

- Die Kostensituation bei funktionalen Anpassungen von Cloud-Services oder deren Integration in bestehende Geschäftsprozesse ist im Vergleich zu den Adaptionskosten herkömmlicher Architekturen weitgehend unbekannt (bzw. muss im Detail unterschieden werden für IaaS, PaaS und SaaS). Aufgrund des hohen Automatisierungsgrads der Cloud-Services sind diese Kosten aber tendenziell höher anzusetzen.
- Massiv skalierende Public-Cloud-Services scheinen zumindest derzeit nicht anpassbar zu sein. Hier sind den Kostenvorteilen im Einkauf etwaige Effizienzverluste in der Nutzung der Standardservices ohne Anpassungen gegenzurechnen. IT-Anwendungen sind als Werkzeug ja nicht nur aus einer Kostensicht im Einkauf, sondern vor allem auch hinsichtlich ihres Beitrags zur Effizienzsteigerung der Geschäftsprozesse zu beurteilen; für dieses Umfeld ungeeignete Prozesse können auch zu Kostensteigerungen führen.
- Zusätzlich zu den zu erwartenden Kostenvorteilen verändert sich bei Public-Cloud-Services für den Auftraggeber des Cloud-Services auch die Kostenstruktur grundlegend. Durch die nutzungsbedingte Verrechnung werden Investitionskosten durch Betriebskosten ersetzt, was entsprechende Auswirkungen auf die Budgetplanung hat. Für Private-Cloud-Services gilt dieses Argument unabhängig von der Größenordnung der Private Cloud bzw. Community Cloud nicht, da hier auch Investitionskosten anfallen. Die Zusammenfassung von mehreren internen Kunden in einer Private Cloud bringt jedoch in Summe mehr Investitionssicherheit für den Cloud Anbieter bei gleichzeitig hoher Flexibilität für die einzelnen Kunden.

Die zu Grunde liegenden wirtschaftlichen Parameter sind aufgrund der zum Teil fehlenden Transparenz des technischen und organisatorischen Modells der CSP schwer zu beurteilen. Abgesehen von entsprechenden vertraglichen Vereinbarungen und SLAs sollten diese Bedenken rund um das Spannungsfeld zwischen Profit und Sicherheit mit in eine Vorab-Klassifizierung über die „Cloud-Fähigkeit“ von Bereichen bzw. Daten einfließen. Es sollte die bestehende Infrastruktur in den Wirtschaftlichkeitsüberlegungen berücksichtigt werden. Die bestehende bzw. für sensible Bereiche auch künftig notwendige Infrastruktur führt zwangsläufig zu Investitionen und Fixkosten, die nicht vermeidbar sind und zusätzlich zu den Kosten der Cloud Services anfallen (Unit costs). Somit können die Vorteile einer Public Cloud nicht unmittelbar auf eine Mischform bzw. mögliche Private Clouds bzw. Community Clouds übertragen werden.

A.3.5 Technische Aspekte und Sicherheit

Technische Aspekte wie Virtualisierung, Provisioning, gemeinsame Nutzung von Ressourcen und Ausgleich von Lastspitzen sind Grundeigenschaften, die Cloud Computing ausmachen. Neben relevanten technischen Aspekten müssen auch Aspekte der IT-Sicherheit bei der Nutzung von Cloud-Lösungen sorgfältig beachtet werden. Relevante technische Aspekte und Sicherheitsaspekte werden in diesem Kapitel behandelt.

A.3.5.1 Technische Aspekte

Bei der Beschreibung von Cloud Computing-Systemen haben sich u.a. die im den folgenden Unterabschnitten beschriebenen technischen Aspekte etabliert.

A.3.5.1.1 Standardisierung

IT-Anwendungen haben in der Regel eine Vielzahl von Schnittstellen bzw. unterhalten Schnittstellen zu anderen Anwendungen. Wären diese Schnittstellen standardisiert, wäre ein Wechsel zwischen Cloud-Anbietern einfach, da notwendiger Anpassungsaufwand geringgehalten werden könnte. Allerdings kann trotz diverser einschlägiger Initiativen nach wie vor nicht von einer breiten Standardisierung im Cloud Computing-Bereich ausgegangen werden. Dementsprechend sind in der Praxis noch immer beträchtliche Projektaufwände bei einem Wechsel zwischen Cloud-Anbietern zu kalkulieren.

Dabei brächte eine verstärkte Compliance mit öffentlichen Standards durchaus auch Chancen mit sich. Beispielsweise könnte sich durch standardisierte Cloud-Umgebungen ein Wettbewerb etablieren, der den Wechsel zwischen Cloud-Anbietern einfacher macht. Standardisierte Schnittstellen sind daher ein wichtiges Kriterium, um eine Abhängigkeit von einzelnen Anbietern (Lock-In) zu vermeiden. Für Standardisierungen im Cloud-Umfeld gibt es bereits eine Reihe von Standards, die durch Cloud-Anbieter idealerweise unterstützt werden sollten. Beispiele sind:

- Open Virtualization Format (OVF)
- Security Assertion Markup Language (SAML)
- OAuth, OpenID Connect
- Service Provisioning Markup Language (SPML)
- Extensible Access Control Markup Language (XACML)
- Liberty Identity Assurance Framework (LIAF)
- Breitere Aktivitäten:
    - NIST Cloud Standard Roadmap, Reference Architecture
    - ETSI TC Cloud

- OASIS Cloud TCs
- DMTF Cloud Standards
- ITU Cloud Standard Roadmap

Darüber hinaus gibt es mit OpenStack eine mehrere Ebenen abdeckende, standardisierte Cloud-Plattform basierend auf offenen Standards, welche üblicherweise in Form von IaaS Anwendung findet. Teilweise wird im Sinne der Interoperabilität eine Kompatibilität zu etablierten, proprietären CSPs und deren Diensten, wie z. B. Amazon EC2 und Google Compute Engine angestrebt. Das Problem des Lock-Ins bleibt jedoch nach wie vor bestehen: Eine anbieterübergreifende, reibungsfreie Migration zwischen unterschiedlichen Angeboten ist somit Stand 2020 im Allgemeinen nicht möglich und nach wie vor mit teilweise erheblichen Aufwänden verbunden. Weiterführende Informationen zu Standardisierungsaktivitäten finden sich unter anderem im Cloud Computing Kompass [CLD-KOM].

A.3.5.1.2 Skalierbarkeit / Elastizität

Unter Skalierbarkeit versteht man im Cloud-Computing-Kontext die (automatische) Anpassbarkeit von Ressourcen an die sich ändernden Leistungsanforderungen von Auftraggebern/Kunden; insbesondere, aber nicht nur bei Lastspitzen (z.B. Dienstbeginn, Tagesabschluss, Monatsabschluss, ...).

Cloud Computing und dessen Grundarchitektur eröffnen hier die Chance, einen Lastausgleich über mehrere Kunden oder Mandanten in der Cloud umzusetzen. Dies kann jedoch gleichzeitig auch zum Risiko werden, falls nicht ausreichend Ressourcen vorgehalten werden. In diesem Fall können alle Kunden oder Mandanten durch unzureichende Ressourcen beeinträchtigt werden.

A.3.5.1.3 ID- und Rechtemanagement

Die Identitäts- und Rechteverwaltung ist wesentlicher Baustein der Zugangskontrolle in Cloud Computing-Systemen. Um etwaige nach wie vor bestehende Sicherheitsbedenken auszuräumen, sind daher die Lösungen der jeweiligen CSP genau zu hinterfragen. Konkret muss frühzeitig abgeklärt werden, wie der CSP mit der Tatsache umgeht, dass seine Administratoren potenziell Zugang zu kritischen Unternehmensdaten haben.

Das ID- und Rechtemanagement muss die sichere Identifikation der Kunden der Cloud selbst, sowie auch die der Administratoren des CSP ermöglichen. Besonders auf die Absicherung der privilegierten Benutzerprofile des CSP muss geachtet werden. Hier muss es dem Kunden der Cloud ermöglicht werden, regelmäßige

Audits (Zugriffe, Zugriffsprofile) durchführen zu können. Für die Authentisierung selbst sollten generell nur starke Verfahren verwendet werden. Die Konnektivität zu einem lokalen IDM (Identity Management) des Kunden ist sicherzustellen, da sonst erhebliche Zusatzaufwände und auch Risiken entstehen können.

Das ID- und Rechtemanagement kann prinzipiell auch bei einem Drittanbieter angesiedelt sein. Sicherheitstechnische Anforderungen an das ID- und Rechtemanagement gelten jedoch auch in diesem Fall.

A.3.5.1.4 Mandantenfähigkeit

Zu den Grundeigenschaften einer Cloud-Architektur zählt die Mandantenfähigkeit (multi-tenancy). Die sichere Mandantenfähigkeit in der Cloud ermöglicht die Partitionierung einer virtualisierten Shared-IT-Infrastructure, wie sie auch bei Server-Virtualisierung in modernen Rechenzentren bereits eingesetzt wird. Dadurch ergibt sich die Chance, verschiedene Anwendungsszenarien (z.B.: Produktions- und Testbetrieb) abzubilden, sowie vergleichsweise einfach zwischen diesen wechseln zu können.

A.3.5.1.5 Sicherheitsarchitektur

Um die Ressourcen von Kunden oder Mandanten (Daten, Anwendungen bzw. Applikationen, Netze, …) zu schützen, ist eine durchgängige Sicherheitsarchitektur zu implementieren. Da Cloud-Systeme mandantenfähig (s.o.) sein müssen, muss auch eine sichere Trennung der Ressourcen von Kunden und/oder Mandanten in der Architektur abgebildet sein.

Neben konventionellen Architekturmodellen zur Realisierung von Sicherheit bietet Secure Access Service EDGE (SASE) ein cloudbasiertes Architekturmodell das auf einer Kombination von Techniken sowie Verfahren basiert, um Sicherheitsrichtlinien durchzusetzen, unerwünschte Inhalte zu blockieren sowie cloud-basiertes Firewall-as-a-Service (FWaaS) sowie vertrauenslose Zugriffe auf Netzwerkressourcen mittels Zero-Trust zum Schutz vor der Anwendung umzusetzen. Für den Fernzugang zu Ressourcen der Organisation wird zumeist auf Verbindungen zurückgegriffen, die mit einem VPN abgesichert sind.

Jeder Zugriff auf Netzwerkressourcen wird individuell authentifiziert und selbst innerhalb definierter Perimeter eines Netzwerks besteht zwischen den Akteuren (sog. „Actors“) wie auch außerhalb der Organisationsgrenzen, kein Vertrauen. Dieser Ansatz beruht auf konstantem Monitoring. Demzufolge handelt es sich bei SASE um eine Konsolidierung einer Vielzahl cloud-basierter Schutzfunktionen zur Verbesserung des Sicherheitslevels.

A.3.5.1.6 Cloud-Management

Um den sicheren Betrieb von Cloud-Services zu gewährleisten, sind vom CSP IT-Managementfunktionen und Prozesse anzubieten, die sowohl die Einrichtung als auch den Betrieb von Cloud-Services unterstützen. CSPs offerieren für ihre Services Werkzeuge in Form von Webportalen, die die benötigten Funktionen zur Verfügung stellen. Typischerweise sind dabei folgende Funktionen inkludiert:

- Steuerung von Services - dazu zählen z.B.
  - Starten,
  - Stoppen oder
  - Reboot.
- Überwachung von Services, um die Leistungsfähigkeit/Leistungsdaten des CSP zu erheben.
- Sicherheitsfunktionen, wie z.B. der sichere Zugriff auf Services, Transparenz von Zugriff und die sichere Identifikation von Kunden und Administratoren des CSP.

Wünschenswert wären zudem Werkzeuge, mit denen die Cloud-Ressourcen und die lokalen on-premise Ressourcen gemeinsam verwaltet werden können.

A.3.5.1.7 Technische Revision

CSP müssen zum Durchsetzen von kundenspezifischen Sicherheitsrichtlinien geeignete Prozesse anbieten. Es muss dem Kunden möglich sein, im Rahmen der Umsetzung seiner Sicherheitspolitik die benötigten Informationen/Zugriffe auf z.B. Log-Dateien oder Zugriffslisten zu haben, um die eigene Compliance zu gewährleisten.

A.3.5.1.8 Patch-Management

Patch-Management umfasst die Planung und Installation von Patches (Software-Updates). Wichtig ist dabei, dass Patches über die gesamte Umgebung zu definierten Zeitpunkten eingespielt werden. Durch die standarisierte Cloud-Infrastruktur ergibt sich die Chance, das Patch-Management bei höherem Effizienzgrad mit geringeren Ausfallzeiten zu bewerkstelligen. Als Schwierigkeit ist der Test auf Verträglichkeit bzw. Kompatibilität von Software-Updates mit kundenspezifischen Anwendungen zu sehen.

A.3.5.2 Zusammenfassung der technischen Aspekte

Die wichtigsten Erkenntnisse aus den vorigen Punkten finden sich überblicksmäßig in der folgenden tabellarischen Zusammenfassung. Für die einzelnen betrachteten Aspekte sind jeweils Chancen und Risiken im Kontext von Cloud Computing zusammengefasst.

	Chance	**Risiken**
Standardisierung	Wettbewerb, Wechsel zwischen Anbietern.	Ohne Standard Abhängigkeit von einzelnen CSP.
Skalierbarkeit	Illusion unbegrenzter Ressourcen beim CSP.	Gleichzeitige Lastspitzen können im schlechtesten Fall zum Stillstand führen.
Identity- und Rechtemanagement	-	Sicherheitsbedenken bei der Umsetzung der CSP, vor allem bei den privilegierten Benutzerkennungen (Administratoren).
Mandantenfähigkeit, Sicherheitsstruktur	Ist eine Kernanforderung an CSP und sollte damit „state of the art“ sein.	-
Cloud Management	Standarddienste (einheitliche Administrationskonsolen) werden durch komfortable Webportale zur Verfügung gestellt.	Einbindung der Werkzeuge an CSPs in kundenspezifische Prozesse noch nicht erprobt.
Technische Revision	-	Auftrennung der kundenspezifischen Daten (Log-Dateien etc.) muss vertraglich geregelt werden. Derzeit noch keine standardisierten Angebote (allerdings z.B. bei PaaS bereits eine Frage des Designs der Applikation).
Patch Management	Schnelles standardisiertes Ausrollen von Patches durch vereinheitlichte Infrastruktur.	Schwierigkeit des Testens der Kompatibilität von Patches, Rücksichtnahme auf kundenspezifische Anforderungen.

A.3.5.3 Sicherheit

Zusätzlich zu den technischen Eigenschaften von Cloud-Diensten wird nachfolgend gesondert auf Sicherheitsaspekte im Cloud-Computing-Kontext eingegangen. Im Gegensatz zur teils rapiden technischen Weiterentwicklung im Cloud-Computing-Bereich, sind die grundsätzlichen Herausforderungen in Bezug auf IT-Sicherheit im Wesentlichen seit Jahren unverändert.

A.3.5.3.1 Informationsschutz

Die Verarbeitung, Speicherung und Übertragung von Informationen muss derart gestaltet sein, dass die Schutzziele der zugehörigen IT-Services eingehalten werden. Dabei sind auch die spezifischen Risiken zentralisierter Infrastruktur zu betrachten.

A.3.5.3.2 Vertraulichkeit

Informationsvertraulichkeit ist dann gegeben, wenn keine unautorisierte Informationsgewinnung möglich ist. Das erfordert die Festlegung von Berechtigungen und Kontrollen, sodass sichergestellt ist, dass Subjekte nicht unautorisiert Kenntnis von Informationen erlangen können. Das umfasst sowohl gespeicherte Daten („data at rest“), als auch Daten, die über ein Netzwerk übertragen werden („data in transit“). Berechtigungen zur Verarbeitung dieser Daten müssen prinzipiell von entsprechenden Administratoren vergeben und entzogen werden können und es müssen Verfahren vorhanden sein, die eine Einhaltung dieser Rechte durchsetzen und überprüfbar machen.

Daten sollen daher zu jedem Zeitpunkt verschlüsselt übertragen bzw. ausgetauscht werden. Auch die Speicherung sollte verschlüsselt erfolgen, um technisch das missbräuchliche Lesen von Daten zu verhindern. Dies ist insbesondere bei der Nutzung von Public Clouds erforderlich und bedingt eine Infrastruktur kryptographischer Dienste, ein entsprechendes Schlüsselmanagement, sowie geeignete Kryptographie-Komponenten. Bis zu einer für den Produktivbetrieb geeigneten Weiterentwicklung der homomorphen Verschlüsselung (d.h. eine berechtigte, beliebige Veränderung des Inhaltes von verschlüsselten Dateien ohne diese zu entschlüsseln) bieten derzeitige Verschlüsselungssysteme und -algorithmen keinen ausreichenden Schutz für ausgelagerte sensible Daten.

Durch die CSP wird nicht immer garantiert, dass Daten verschlüsselt auf einem Speichermedium vorliegen. In den Geschäftsbedingungen der meisten CSP gibt es keine Zusicherungen darüber, wo Daten gespeichert werden und wie ihre Vertraulichkeit geschützt wird. Häufig bleibt es dem Kunden selbst überlassen, entsprechende Sicherheitsverfahren anzuwenden.

Die notwendigen Skaleneffekte eines CSP können nur durch einen sehr effizienten IT-Management-Prozess erreicht werden. Aus diesem Grund muss die Administration virtueller Server per Zugriff auf die Virtualisierungsschicht durchgeführt werden. Eine größere Anzahl an Personen hat Zugriff auf die vom CSP zur Verfügung gestellten virtuellen Maschinen und die zugehörigen Netze, sodass das Risiko des unautorisierten Zugriffs signifikant höher ist als in traditionellen IT-Umgebungen.

Aus Optimierungsgründen haben CSPs die Möglichkeit, Daten und Services auch zu anderen CSPs auszulagern. Dadurch entstehen neue Abhängigkeiten und Risiken in Bezug auf Informationsvertraulichkeit, die entsprechend bewertet werden müssen.

Generell muss die Vertraulichkeit der Daten für den gesamten Daten-Lebenszyklus sichergestellt werden, d.h. von der Erfassung der Daten über deren Nutzung und Archivierung bis hin zum Löschen. Da die Daten in beliebigen Teilsystemen einer Cloud gehalten werden, ist nur sehr schwer nachvollziehbar, ob die ausgelagerten Daten in der Cloud tatsächlich vollständig gelöscht sind (Backupkopien, Replikationen beim Anbieter).

A.3.5.3.3 Integrität

Ein System gewährleistet Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Die Integrität von Daten, Nachrichten und Informationen bezeichnet somit deren Unverfälschtheit.

Das Ziel der Datenintegrität sollte nicht nur der Cloud-Service selbst erfüllen, sondern muss auch von allen weiteren beteiligten Komponenten eines Cloud Computing-Systems sichergestellt werden. Der CSP ist für die Integrität des Systems und der Services vollinhaltlich verantwortlich. Dies sollte auch vertraglich festgehalten werden.

Gespeicherte Daten müssen vor nicht autorisierten Manipulationen geschützt werden. Fehler in der Systemkonfiguration des Anbieters können zu einer Integritätsverletzung führen. Die Daten in Cloud Computing-Systemen sollten zudem immer mit einer kryptografischen Prüfsumme versehen werden, wobei die Originalprüfsumme bei einem vertrauenswürdigen Dritten zum Vergleich hinterlegt werden kann. Diese sollte bei jedem Zugriff auf Daten in Cloud-Computing-Systemen überprüft werden, um Integritätsverletzungen feststellen zu können. Dieses Verfahren verursacht jedoch einen zusätzlichen Kommunikationsaufwand und erhöht insgesamt die Komplexität.

Neben der Datenintegrität sind in Cloud-Systemen auch die Softwareintegrität, Konfigurationsintegrität und Nachrichtenintegrität wichtig und dementsprechend sicherzustellen:

- Softwareintegrität stellt sicher, dass die eingesetzte Software, um ein Cloud-Computing-System zu betreiben, intakt vom Softwarehersteller geliefert wurde und beispielsweise keine Hintertüren und ähnliche Verfälschungen aufweist.
- Konfigurationsintegrität stellt sicher, dass die Konfiguration einer Cloud-Ressource oder eines Cloud-Service nur durch autorisierte Personen geändert werden kann. Dies ist in Cloud-Systemen besonders wichtig, da eine Cloud-Umgebung meist automatisiert über Konfigurationsskripte aufgesetzt und verwaltet wird.

- Nachrichtenintegrität ist eine weitere wichtige Anforderung, die sowohl innerhalb einer Cloud als auch zwischen verschiedenen Clouds und den Systemen des Benutzers sichergestellt werden muss. Neben der Nachrichtenintegrität bedürfen auch Verwaltungs- und Steuerinformationen besonderem Schutz, da auch diese Nachrichten häufig über ein öffentliches Netzwerk transportiert werden.

A.3.5.3.4 Verfügbarkeit

Die Verfügbarkeit gibt an, dass Funktionen eines IT-Service ständig bzw. innerhalb einer vorgegebenen Zeit, die von Service zu Service unterschiedlich sein kann, zur Verfügung stehen. Die Verfügbarkeit kann über verschiedene Maßnahmen erhöht bzw. gewährleistet werden. Dazu zählen logische Schutzmaßnahmen wie Zugriffsrechte ebenso wie technische Maßnahmen wie beispielsweise Redundanzen oder auch Schutz vor gezielten Sabotageversuchen Dritter. Cloud Computing bietet den Vorteil, dass standardisierte Ressourcen dynamisch skalieren und zur Sicherstellung der Verfügbarkeit gezielt an andere Stellen der Cloud umverteilt werden können. Dabei wird die Netzwerkverfügbarkeit immer wichtiger.

A.3.5.3.5 Authentizität

Authentizität bezeichnet die Echtheit, Zuverlässigkeit und Glaubwürdigkeit eines Objekts. Dadurch wird sichergestellt, dass die Herkunft des Objekts zweifelsfrei nachgewiesen werden kann. Eine Möglichkeit für den technischen Nachweis von Authentizität ist die digitale Signatur.

A.3.5.3.6 IT-Sicherheit im Kontext von Cloud Computing

Cloud Computing bietet besonders für die IT-Sicherheit erhebliche Chancen, aber auch ungleich viel mehr Risiken. Positive Effekte sind dabei Standardisierung und Skalierbarkeit, demgegenüber stehen unter anderem die negativen Effekte wie Datenlokation, Kontrollverlust von Daten, etc. Um einen langfristigen Erfolg von Cloud Computing auch in sicherheitskritischen Szenarien sicherzustellen, ist die Betrachtung kritischer Erfolgsfaktoren, allen voran das Thema IT-Sicherheit, besonders bedeutsam.

Der Einsatz von Cloud-Services verändert traditionelle IT-Infrastrukturen. So ist die skalierbare, flexible und zentrale Bereitstellung von Sicherheitsfunktionen und Sicherheitsmaßnahmen möglich und schafft auf diese Weise die Voraussetzung zur bedarfsgesteuerten Erfüllung differenzierter Sicherheitsanforderungen – gleichzeitig bleiben aber andere Aspekte der IT-Sicherheit, wie etwa die Anwendung von Verschlüsselung, problematisch.

Je nach Servicemodell muss von unterschiedlichen Bedrohungsszenarien ausgegangen werden. Diese sollen in gesonderten Risikoanalysen betrachtet werden:

- Infrastruktur-Provider (IaaS) bieten Sicherheitsfeatures lediglich auf Hardware bzw. Infrastrukturebene an. Für das Management und die Umsetzung der darüberhinausgehenden Sicherheitsmaßnahmen ist der Kunde verantwortlich.
- Bei PaaS zeichnet der Anbieter für Sicherheitsfunktionen von Plattformdiensten, wie z. B. Datenbanken und Middleware, verantwortlich.
- SaaS-Provider regeln Details der Applikationsnutzung vertraglich, beispielsweise geltende Service Level, Sicherheit und Compliance.

A.3.5.3.7 Bedrohungen

Bedrohungsszenarien betreffen traditionelle IT-Konzepte und Cloud-Computing-Modelle gleichermaßen. Die hier skizzierten Bedrohungen stellen die häufigsten Gefahren dar, ohne den Anspruch auf Vollständigkeit zu erheben. Es muss daher im konkreten Fall eine spezifische Bedrohungsanalyse erstellt werden.

Generell können zwei grundlegende Arten von Bedrohungen unterschieden werden. Zum einen können Bedrohungen die verarbeiteten, gespeicherten und übertragenen Daten selbst betreffen. Zum anderen existieren Bedrohungen auch für die (Cloud-)Services, die diese Daten und Informationen verarbeiten. Im Sinne einer ganzheitlichen Betrachtung müssen beide Arten von Bedrohungen berücksichtigt werden.

Um mit Bedrohungen betreffend Daten und Informationen geeignet umgehen zu können, empfiehlt sich eine Kategorisierung von Daten entsprechend ihrem Schutzbedarf. Im öffentlichen Sektor werden Daten nach Informationssicherheitsgesetz (InfoSiG) in Klassifizierungsstufen (unklassifiziert, eingeschränkt, vertraulich, geheim, streng geheim) eingeteilt, und müssen je nach Stufe einer unterschiedlichen Behandlung zugeführt werden, um potenziellen Bedrohungen geeignet zu begegnen. Informationen, welche als z.B. geheim klassifiziert werden, sind von einer Bearbeitung in einer Public Cloud ausgeschlossen, da eine lückenlose Kontrolle des Zugriffs in so einer Umgebung nicht mehr gewährleistet ist. Daten, welche nach InfoSiG klassifiziert sind, dürfen somit nur mehr in einer Private Cloud bzw. Community Cloud verarbeitet werden. Hierbei ist besonders zu berücksichtigen, dass dies Daten der Kategorien vertraulich und geheim umfasst. Streng geheime Daten nach InfoSiV §9(2) dürfen in jedem Fall nur auf nicht vernetzten und abstrahlungsarmen Geräten verarbeitet werden.

Bedrohungen die Cloud-Services selbst betreffend drehen sich primär um den Aspekt der Verfügbarkeit. Alle Services, die von einem Cloud-Anbieter angeboten werden (XaaS), unterliegen einer ständigen potenziellen DoS-Gefahr (Denial of Service). Daneben müssen jedoch auch Bedrohungen in Bezug auf andere Schutzziele wie Vertraulichkeit berücksichtigt werden, existiert bei Cloud-Lösungen doch die immanente Gefahr des unberechtigten Datenabflusses an Dritte.

Eine besondere Relevanz im Cloud-Umfeld haben Bedrohungen in Bezug auf Social Engineering. Social Engineering bezeichnet eine Angriffsklasse, bei der Personen mit entsprechenden (Zugriffs)rechten dazu verleitet werden, Zugangsdaten-, verfahren, o.ä. preiszugeben. Im Cloud-Bereich ist Social Engineering eine noch größere Gefahr als in traditionellen Szenarien, da Administratoren der CSPs ein attraktives Angriffsziel darstellen können und ein erfolgreicher Angriff die Daten und Dienste vieler an sich voneinander unabhängiger Kunden betreffen kann. Zur Mitigation dieser Bedrohung sind Ansprechpersonen und Prozesse zu definieren, um bei einem Sicherheitsvorfall sowohl auf strukturierte Abläufe zurückgreifen als auch Zuständigkeiten abgrenzen zu können.

A.3.5.3.8 Standards und Normen

Zurzeit sind Cloud-Service-Provider kaum nach einschlägigen Normen zertifiziert (z.B.: ISO2700X, ISO 27018, ISO 27019, BSI Grundschutz, BASEL III). Bei der Einholung von Angeboten von CSP ist also auf derartige Zertifizierungen besonders Wert zu legen. Relevante Normen und Standards sind unter anderem im Cloud Computing Kompass [CLD-KOM] gelistet und umfassen u.a. folgende Auditing-/ Zertifizierungsinitiativen und Tools:

- CloudAudit/Cloud Controls Matrix (Cloud Security Alliance)
- StarAudit (EuroCloud)
- ISACA Cloud Computing Management Audit/Assurance Program
- NIST SP 800-53, NIST SP 800-144, SP 800-30
- Cloud Auditing Data Federation (DMTF)
- Deloitte Cloud Computing Risk Intelligence Map
- Federal Risk and Authorization Management Program - (FedRAMP)

A.3.6 Auswirkungen von Cloud Computing auf Geschäftsprozesse

Die Einführung und Verwendung von Cloud Computing in einem Unternehmen oder einer Organisation hat weitreichende Auswirkungen bis hin auf Geschäftsprozessebene. Relevante damit im Zusammenhang stehende Aspekte werden in diesem Abschnitt diskutiert.

A.3.6.1 Grundsätzliches

Cloud Computing als IT-Betriebsmodell ist nicht nur für IT-Abteilungen von Bedeutung, sondern für Unternehmen und die öffentliche Verwaltung insgesamt eine relevante Herausforderung. Durch den Einsatz von Cloud Computing kann eine ganzheitliche Änderung von Unternehmensstrategien und -strukturen erforderlich werden. Die Auslagerung von Teilen der eigenen Geschäftsprozesse an einen Dritten (CSP) ist mit signifikanten Änderungen in diesen Prozessen verbunden. Eine mögliche Folge ist die Notwendigkeit der Umverteilung von Rollen und Kompetenzen und damit Prozessen.

Die Zusammenarbeit von internen Prozessen und den Prozessen des CSP sind in einem Cloud Compliance Regelwerk (im Rahmen einer Dienstleistervereinbarung) transparent festzulegen und zu kontrollieren. Im Sinne der Aufgabendefinition und Aufgabenüberwachung wird auch in diesem Zusammenhang auf die Notwendigkeit des Abschlusses ausreichender Service Level Vereinbarungen (SLAs) und Operational Level Vereinbarungen (OLAs) verwiesen.

A.3.6.2 Strategische Aspekte der Prozessveränderung durch Cloud Computing

Prinzipiell verfügen viele bestehende Anwendungen, die nicht als Cloud-Service bezeichnet werden, über die typischen Anforderungen und Charakteristika von Cloud-Services (z.B. gemeinsame Nutzung von Ressourcen über Vernetzung, Lizenzgebühren für die Nutzung statt Investitionen in eigene Infrastruktur, Standardisierung). Bestehende Erfahrungen aus der Nutzung solcher Anwendungen, speziell im Zusammenhang mit Betrieb und Datenspeicherung über einen Dienstleister und bei Anpassungen von Prozessen können auch bei der Evaluierung von potenziellen Cloud-Services genützt werden.

Standardisierung ist der wesentlichste Faktor für Kostenersparnisse beim Einsatz von Cloud Computing. Spezifische Cloud-Anwendungen sind ein Werkzeug zur effizienten Umsetzung dieser Standardisierung. Gerade Public Cloud-Services unterliegen einem sehr hohen Standardisierungszwang, der bei einem Private Cloud-Service nicht immer gegeben ist. Entsprechend dem Grad der Standardisierung der gewählten Cloud-Lösung ist mit Änderungen in den Geschäftsprozessen und unterschiedlichen Kosten und Finanzierungsrisiken zu rechnen. Bei einem Einsatz von Cloud-Services unterschiedlicher Dienstleister muss Interoperabilität zur Sicherstellung der Unabhängigkeit von einem bestimmten Anbieter in den Prozessen berücksichtigt werden. Bei Nutzung standardisierter Cloud-Lösungen sollte durch den flexiblen Einsatz von Rechenleistung schnell auf Änderungen in den Geschäftsprozessen reagiert werden können.

Compliance- und Governance-Prozesse werden in Unternehmen und der öffentlichen Verwaltung mit steigendem Einsatz von Cloud-Services externer Dienstleister durch die Notwendigkeit der Sicherstellung und Kontrolle der Einhaltung von Datensicherheit und Rechtskonformität an Bedeutung gewinnen. Neben der gründlichen Ausarbeitung von SLAs zur Abdeckung der Anforderungen bei der Nutzung eines Cloud-Services müssen auch die dazugehörigen Kontrollprozesse ausreichend definiert und umgesetzt werden.

A.3.6.3 Cloud Compliance

Das hohe Maß an Abhängigkeit zwischen Cloud-Service-Anbietern und Nutzern und die dadurch verzahnten Prozesse und Verantwortlichkeiten erfordern ein stabiles Regelwerk, das vielfach unter dem Begriff „Cloud Compliance“ [BITK10] zusammengefasst wird. Cloud Compliance hat zum Ziel, Transparenz und Sicherheit für alle Anspruchsgruppen (Stakeholder) zu schaffen und bietet damit eine wichtige Basis, um alle Vorteile von Cloud Computing für Anbieter, Kunden und Endnutzer vollumfänglich nutzbar zu machen.

Der Begriff Cloud Compliance bezeichnet die nachweisbare Einhaltung von Regeln zur Nutzung oder Bereitstellung von Services über Cloud Computing. Zur Bestätigung der Cloud Compliance können sich Anbieter zertifizieren lassen. Zu den verschiedenen Zertifikaten/Gütesiegeln zählen das Gütesiegel SaaS von EuroCloud, Trusted Cloud, CSA STAR, TÜV Trust IT und das IT-Grundschutz-Zertifikat des BSI. Eine Zertifizierung allein reicht jedoch nicht für eine abschließende Beurteilung eines Cloud-Anbieters oder seines Angebots in Hinblick auf die Anforderungen der Cloud Compliance aus.

A.3.6.4 Entscheidungskriterien zur Auswahl von Cloud-affinen Anwendungen und Services

Unbedingt zu beachten ist, dass die Betrachtung der Unternehmensgröße nur einen einzelnen Parameter in einer Vielzahl von Entscheidungsparametern darstellt. Anhand der folgenden Grafik soll als Entscheidungshilfe ein Überblick gegeben werden, der zeigt, welche Cloud-Typen welche Kriterien erfüllen.

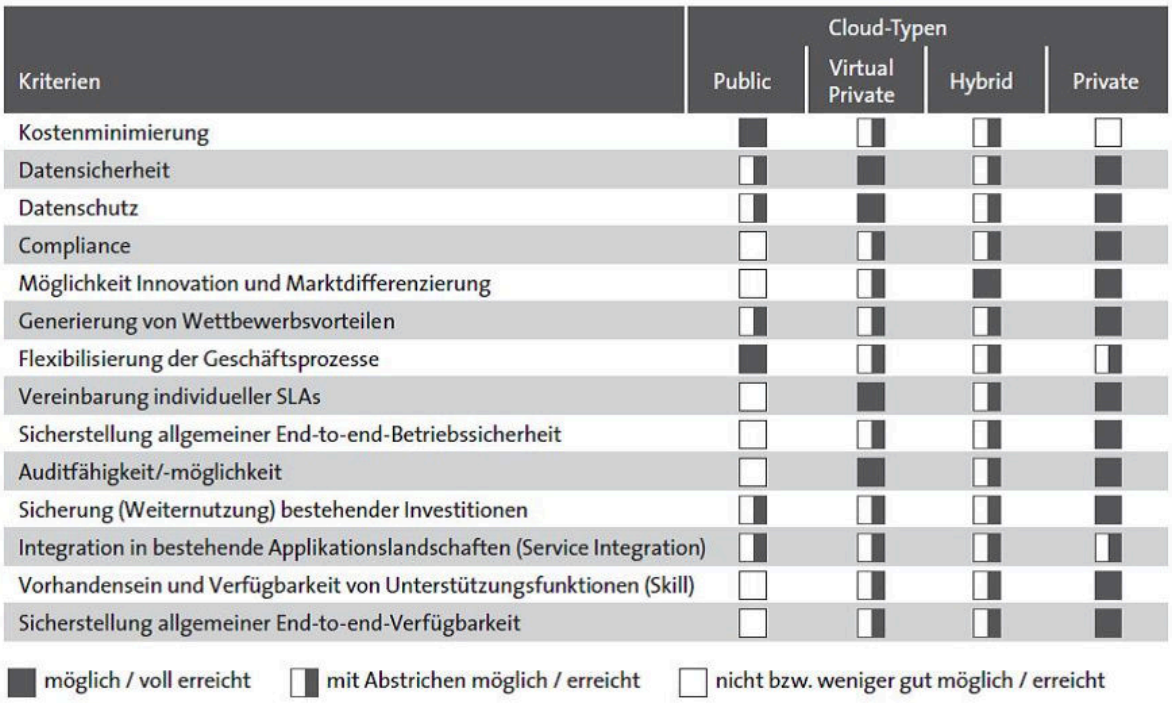

Abbildung A.3.1: Bewertung der Cloudtypen

Die Integrationsfähigkeit von Cloud-Services in eine Gesamtorganisation und Gesamt-IT-Landschaft ist eine der wesentlichsten Entscheidungskriterien. Dies wird durch das Ergebnis einer von Forrester präsentierten Umfrage unterstrichen, die bei jenen Entscheidungsträgern, die bereits mit Cloud-Services vertraut sind, das Thema „Integration“ als größte Herausforderung identifiziert hat.

Einen wichtigen Spezialfall stellt die Nutzung von Cloud Computing für Desktop-Services (z.B. Office-Anwendungen, …) dar: Via Cloud Computing werden Arbeitsplatz-Systeme situativ an die aktuellen Notwendigkeiten des Nutzers angepasst. Da die Anwendungen und Daten auf Medien in der Cloud vorgehalten werden, ist der Defekt eines portablen Endgeräts unbedeutend (BITKOM).

A.3.6.5 Mögliche Cloud Services im öffentlichen Sektor

Auch im öffentlichen Sektor ergeben sich für Cloud Computing diverse Anwendungsmöglichkeiten. Exemplarische Anregungen für mögliche Cloud-Services im Umfeld öffentlicher Behörden werden in den folgenden Paragrafen gelistet:

- Infrastructure-as-a-Service (IaaS):
  - Archivierung von Daten
  - Backup von Daten
  - Rechenleistung und Speicherbedarf

    - Virtuelle Server
- Platform-as-a-Service (PaaS):
    - Plattform für das Abbilden von behördeninternen und/oder bürgerorientierten Prozessen (elektronischen Formularen)
    - Plattform zum einfachen Erstellen von Web-Applikationen; diese Plattform bindet über einfache Module (APIs) die E-Government-Infrastruktur mit ein (z.B. Zustellung, Payment, sichere Identifizierung und Authentifizierung, SZR-Services, etc.)
    - Datenbanken
- Software-as-a-Service (SaaS):
    - Desktop-Software wird als cloudbasierter Dienst angeboten - Zugriff erfolgt bspw. über Web-Browser
    - Workflow Management System, wie bspw. elektronische Aktensysteme
    - Collaboration Suite
    - *Identity-Management-as-a-Service*: die sichere Authentifizierung von Benutzerinnen und Benutzern über nationale E-ID-Systeme wird nach dem Muster eines Identity Providers als "zentrale" Infrastruktur angeboten.
    - *Security-as-a-Service*: Mail-Filter (Filtern auf SPAM und Malware etc.) kann performant als Cloud-basierter Dienst angeboten werden.

A.3.6.6 Analyse-Logik für die Auswahl von Cloud-kompatiblen Services

Bei der Analyse und Auswahl von IT-Komponenten und Services, die für eine Migration in die Cloud in Frage kommen, müssen prinzipiell folgende Faktoren berücksichtigt werden:

- rechtliche Aspekte (siehe dazu Kapitel A.3.2)
- (wirtschaftliche) Vorteilhaftigkeit
- Steuerbarkeit
- Risikobeherrschbarkeit

Die Faktoren und die mit diesen Faktoren verknüpften Detailaspekte, die auch in diesem Anhang detaillierter ausgeführt wurden, müssen Grundlage für Entscheidungen zur Nutzung von Cloud Computing sein.

Im Allgemeinen ist die Entscheidungsfindung bezüglich der Nutzung von Cloud Computing nicht immer einfach, da sehr viele unterschiedliche Faktoren und Aspekte in Betracht gezogen werden müssen. Sinnvoll kann daher ein schrittweises Vorgehen sein, bei dem zunächst jene IT-Komponenten und Services in die Cloud migriert werden, für die die Vorteile aus einer Cloud-Migration offensichtlich überwiegen.

Zum Beispiel sind IaaS und PaaS für Test- und Entwicklungsserver sowohl für Private als auch für Public Cloud-Lösungen die am einfachsten einzuführenden Services (allerdings immer unter der Gesamtbetrachtung der **Sinnhaftigkeit**, **Wirtschaftlichkeit** und der **verwendeten Testdaten**). Ein anderes Beispiel wäre die öffentliche Publikation von unkritischen Daten/Inhalten über das Internet: Auch hier könnten IaaS oder PaaS Cloud Services genutzt werden.

Zudem können vertikale Services mit Cloud-Potenzial bzw. mit bereits Cloud-ähnlicher Realisierung unmittelbar auf ihre technische Realisierung hin überprüft werden, um festzustellen, ob alle technischen Trends moderner Cloud-Services sinnvoll aufgenommen wurden.

Horizontale branchenunabhängige Service-Kandidaten bedürfen hingegen der Evaluierung auf Integrationsbedarf, um bestehende Service-Integrationen und Prozessoptimierungen nicht zu verlieren und sie bedürfen einer politischen Willensbildung, ob sie „betriebskritisch“ sind und aufgrund dieser Kritikalität ein Auslagern zu einem bestimmten Public oder Private Cloud-Anbieter politisch erwünscht ist.

Allen Varianten gemeinsam ist die nötige kritische Gesamtkostenbeurteilung zur letztgültigen Entscheidungsfindung, ob ein Cloud Service sinnvoll genutzt werden kann oder eben nicht.

A.3.7 Entscheidungsfindungsprozess

Bevor man eine Entscheidung für die Nutzung von Cloud Computing trifft oder ein spezielles Modell auswählt, müssen Entscheidungsgrundlagen geschaffen werden. In diesem Zusammenhang sind jedenfalls folgende organisatorischen, rechtlichen und technischen Punkte zu klären, für Details sei auf die entsprechenden Kapitel dieses Anhangs verwiesen.

A.3.7.1 Anforderungen

Organisatorische Anforderungen

- Ab wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden? Wann ist der Schwellenwert für Ausfallzeiten erreicht?
- Welche Daten disqualifizieren eine IT-Anwendung aufgrund der besonderen Sensitivität?
- Welche Risiken sind für eine Organisation aufgrund von Service-Ausfällen tragbar?
- Hat eine IT-Anwendung zu viele Abhängigkeiten, um sinnvoll in eine Cloud ausgelagert zu werden?

- Was ist der maximal tolerierbare Aufwand für die Migration eines Verfahrens in die Cloud? Steht dies in Verhältnis zu den erwarteten Einsparungen?
- Wie hoch ist die Dauer des Return on Investment inkl. der Transitionskosten?

Rechtliche Anforderungen

- Werden personenbezogene Daten verarbeitet?
- Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, für die ein Angemessenheitsbeschluss der Kommission vorliegt, verarbeitet oder liegen sonstige geeignete Garantien oder Verarbeitungsgründe vor?
- Bietet der Auftragsverarbeiter hinreichende Garantien, dass ausreichende organisatorische und technische Maßnahmen gesetzt sind sowie Fachwissen, Kompetenz, Zuverlässigkeit und dergleichen bestehen, um den Anforderungen der DSGVO und des DSG gerecht zu werden?
- Führt der Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten?
- Wurde vom Auftragsverarbeiter ein Datenschutzbeauftragter bestellt?
- Werden Subauftragnehmer beauftragt und gilt für diese Gleiches wie für den Auftragsverarbeiter?
- Nimmt der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter in Anspruch, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen?
- Erfolgt die Verarbeitung auf Grundlage eines Vertrages oder eines anderen in im DSG genannten Rechtsinstruments der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind?
- Stellt der Auftragsverarbeiter die Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO sicher?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zur Pseudonymisierung oder Verschlüsselung personenbezogener Daten?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen gegen den Verlust oder unbefugtem Zugriff auf die Daten?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zur Protokollierung der Zugriffe?
- Hält der Auftragsverarbeiter die Grundsätze des Datenschutzes durch Technik (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default) durch entsprechende Maßnahmen ein?
- Ist beim Auftragsverarbeiter ein Prozess implementiert, der die regelmäßige und anlassbezogene Evaluierung der Datensicherheitsmaßnahmen sicherstellt?

- Ist sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen, die Einschränkung der Verarbeitung oder die Übertragung der Daten der Betroffenen in der Cloud gemäß den rechtlichen Vorgaben gewährleistet und durchführbar?
- Gibt es ein Regelwerk, das das Verfahren zur Wahrung der Rechte der Betroffenen im Fall von gemeinsam Verantwortlichen klar regelt?
- Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)?
- Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten?
- Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)?
- Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Backup) erhalten bleiben?
- Gibt es ein Regelwerk, wonach die Zurückstellung (inkl. Löschung der Daten beim CSP) an den Verantwortlichen nach Beendigung des Vertragsverhältnisses erfolgt?
- Ist bei Datenschutzverletzungen ein Meldeprozess bei Verantwortlichem und Auftragsverarbeiter etabliert?
- Können innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden erfüllt werden?

Technische Anforderungen

- Werden die im Einsatz befindlichen Schnittstellen unterstützt?
- Werden starke Identifizierungs- und Authentifizierungsverfahren für Cloud-Kunden und Administratoren genutzt?
- Ist eine durchgängige Sicherheitsarchitektur implementiert?
- Können die für die Umsetzung der eigenen Sicherheitspolitik benötigten Zugriffe (z.B. Log Dateien, Zugriffslisten) gewährt werden?
- Können Patches getestet werden und aus Kompatibilitätsgründen zurückgehalten werden?
- Stellen kryptografische Methoden die Integrität der Daten sicher?
- Welche Verfügbarkeiten können garantiert werden?
- Wie skaliert die Cloud-Lösung?
- Wie wird der Wechsel von einem Cloud-Anbieter zu einem anderen ermöglicht?

A.4 Smartphone Sicherheit

Smartphones konnten sich in den letzten Jahren zunehmend als präferierte Endnutzergeräte etablieren und lösten vor allem im privaten Bereich Desktop-PCs und Laptops als Mittel der Wahl zur Konsumierung digitaler Inhalte ab. Auch im professionellen Umfeld gewinnen Smartphones stetig an Bedeutung und sind mittlerweile oft fixer Bestandteil der IT-Infrastruktur von Unternehmen. Aufgrund ihrer technischen Eigenschaften und der im Vergleich zu klassischen Endnutzergeräten punktuell divergierenden Anwendungsszenarien bietet die Verwendung von Smartphones für Unternehmen einerseits vielfältige Möglichkeiten, birgt andererseits jedoch auch diverse spezifische Risiken. Der geplante Einsatz von Smartphones im Unternehmensumfeld bedarf daher einer detaillierten Sicherheits- und Risikoanalyse, in der mögliche Bedrohungen identifiziert und geeignete Gegenmaßnahmen erarbeitet werden. Dieser Anhang soll dabei unterstützen, indem er sowohl plattformunabhängige Bedrohungen als auch plattformspezifische Bedrohungen diskutiert und entsprechende Gegenmaßnahmen aufzeigt.

Dieses Kapitel basiert auf unterschiedlichen Arbeiten, Studien und Analysen die A-SIT und EGIZ durchgeführt haben. Grundlegend für dieses Kapitel ist folgendes Dokument:

- Bedrohungsanalyse und Sicherheitsanforderungen für M-Government Applikationen (Thomas Zefferer, Peter Teufl)

A.4.1 Grundlagen

Ziel dieses Anhangs ist es, relevante Sicherheitsaspekte, die sich bei einem Einsatz von Smartphones im Unternehmensumfeld ergeben, möglichst systematisch zu betrachten. Auf diese Weise sollen einerseits Möglichkeiten dieser Technologie aufgezeigt und andererseits damit im Zusammenhang stehende Bedrohungen und mögliche Gegenmaßnahmen erläutert werden.

Als Grundlage für diese systematische Betrachtung von Möglichkeiten, Bedrohungen und Gegenmaßnahmen definiert dieser Abschnitt zunächst im Überblick die Komponenten einer Smartphone-Infrastruktur, identifiziert deren relevante Assets, geht auf Sicherheitsaspekte moderner Smartphones ein, listet mögliche Angriffsarten und skizziert überblickmäßig mögliche Gegenmaßnahmen. Damit stellt dieser Abschnitt die Grundlage für nachfolgende Abschnitte dar, in denen auf einzelne Detailaspekte detaillierter eingegangen wird.

A.4.1.1 Komponenten einer Smartphone-Infrastruktur

Abbildung A.4.1 zeigt ein allgemeines Modell einer Smartphone-Infrastruktur, wie sie üblicherweise in Unternehmen umgesetzt ist. Das Modell ist bewusst abstrakt gehalten und blendet spezifischere Umsetzungsdetails aus, sodass dieses als allgemeingültige Basis für eine systematische Betrachtung fungieren kann. Die einzelnen Elemente des dargestellten Modells sind nachfolgend beschrieben.

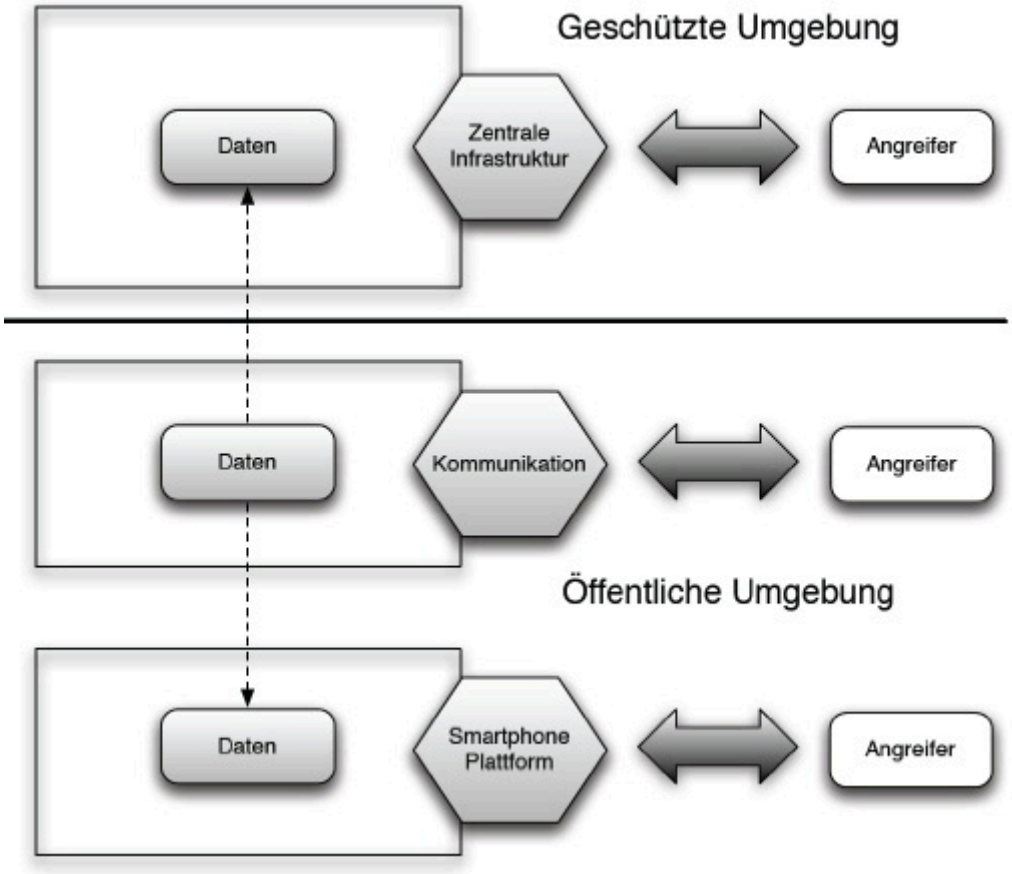

Abbildung A.4.1: Hauptkomponenten einer Smartphone Infrastruktur

Wie in Abbildung A.4.1 dargestellt, kann in Bezug auf eine Smartphone-Infrastruktur eines Unternehmens zwischen zwei Umgebungen unterschieden werden:

- **Geschützte Umgebung:** Die geschützte Umgebung umfasst alle Komponenten eines Unternehmens oder einer Behörde, die sich innerhalb einer geschützten Infrastruktur befinden. Zum Schutz dieser Infrastruktur und ihrer Komponenten kommen sowohl organisatorische als auch technische Maßnahmen zum Einsatz.
    - **Technische Maßnahmen:** Technische Maßnahmen umfassen physische Vorkehrungen wie Gebäudeschutz, Schließsysteme oder Wachpersonal. Daneben kommen üblicherweise auch IT-Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systeme, Netzwerktrennung oder Methoden der sicheren Benutzerauthentifizierung zur Anwendung.

    - **Organisatorische Maßnahmen:** Zu den organisatorischen Maßnahmen zum Schutz sicherer Infrastrukturen gehören allgemeine Verhaltensregeln (Policies), Schulungen und Vorschriften.
- **Öffentliche Umgebung:** In dieser Umgebung können üblicherweise viele der oben genannten technischen und organisatorischen Maßnahmen, die in einer geschützten Umgebung zur Anwendung kommen, nicht mehr verwendet werden. Aufgrund seiner inhärenten Mobilität kann beispielsweise ein Smartphone an nahezu jedem beliebigen Ort eingesetzt werden und ist somit eindeutig der öffentlichen Umgebung zuzuordnen. Für Sicherheitsüberlegungen relevant ist darüber hinaus auch die Tatsache, dass Smartphones meist sowohl im geschäftlichen als auch im privaten Umfeld verwendet werden.

Neben dieser Unterteilung in geschützte und öffentliche Umgebungen können für Smartphone-Infrastrukturen außerdem die folgenden drei Hauptbereiche identifiziert werden:

- **Zentrale Infrastruktur** Die zentrale Infrastruktur befindet sich in der geschützten Umgebung und enthält unter anderem die folgenden Komponenten, die für die Sicherheit eines Systems von Bedeutung sind:
    - **Daten:** Dabei handelt es sich um alle kritischen Daten, die für einen Angreifer von Interesse sein könnten.
    - **Dienste:** Dienste erlauben den Zugriff auf zentral verfügbare Daten und können sowohl für die interne als auch für eine öffentliche Verwendung zur Verfügung stehen.
    - **Zugriffspunkte auf zentrale Dienste:** Unabhängig von der jeweiligen Smartphone-Plattform wird für die Kommunikation mit internen Services meist ein zentraler Zugriffspunkt (Backend, Micro Services, etc.) genutzt, der den Austausch von Daten mit diesen Services ermöglicht.
- **Kommunikation:** Der Austausch von Daten erfolgt meistens über öffentliche Netze wie dem Internet. Es können sämtliche Schichten des OSI-Referenzmodells dabei zum Einsatz kommen.
- **Smartphone-Plattform:** Die Smartphone-Plattform selbst wird aufgrund ihrer Mobilität ebenfalls der öffentlichen Umgebung zugeordnet und enthält folgende sicherheitsrelevanten Komponenten:
    - **Daten:** Abgesehen von den auf dem Smartphone befindlichen Daten, können mittels Smartphones neue Daten gesammelt werden.
    - **Betriebssystem:** Das Betriebssystem des Smartphones. Aktuell sind hier die Betriebssysteme Android und iOS vorherrschend.
    - **Kommunikationsschnittstellen wie Bluetooth, NFC, WLAN, GSM, GPRS, UMTS (3G), LTE (4G), 5G:** Diese Kommunikationsschnittstellen erlauben dem Smartphone die drahtlose Kommunikation mit Netzwerken und anderen Geräten.

- **Applikationen (Apps):** Neben der mit dem Betriebssystem ausgelieferten Funktionen können Software-Features eines Smartphones über Apps nahezu beliebig erweitert werden.
- **Sensoren:** Smartphones verfügen über eine Vielzahl an Sensoren, deren Daten (Position, Lage, Beschleunigung, Ton, Bild, etc.) u.a. auch von installierten Apps verwendet werden können.
- **Hardware Security Module:** Diverse Smartphones verfügen über speziell gehärtete Hardware, die zur sicheren Speicherung und Verwendung kryptographischen Schlüsselmaterials verwendet werden kann.

Angriffe, die Daten in diesen Bereichen zum Ziel haben, können naturgemäß in all diesen Umgebungen stattfinden. Dementsprechend müssen Bedrohungsszenarien in allen Umgebungen und Bereichen berücksichtigt werden.

A.4.1.2 Assets einer Smartphone Infrastruktur

Daten sind als Kern-Asset (Primär-Assets) zu sehen. Ziel von Angriffen ist es meist, Zugriff auf geheime, vertrauliche, private oder sicherheitskritische Daten zu erlangen. Abgesehen davon kann Ziel eines Angriffs auch sein, Kontrolle über das Smartphone zu erlangen, um bspw. Daten zu sammeln oder durch ungewollte Verschlüsselung dieser Daten Lösegeld zu erpressen.

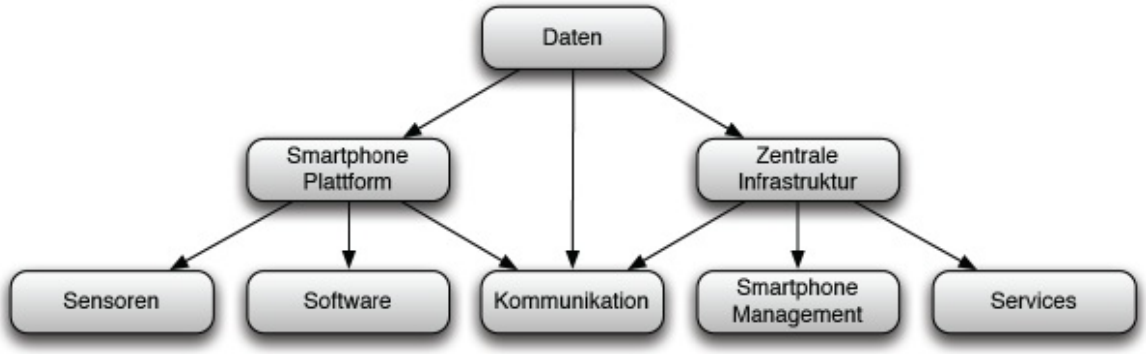

Abbildung A.4.2: Relevante Komponenten zum Schutz des Kern-Assets Daten

Neben Daten als Primär-Assets existieren in einer Smartphone-Infrastruktur noch eine Reihe sogenannter Sekundär-Assets. Diese haben für sich nur einen beschränkten Wert, allerdings hat deren Sicherheit einen direkten oder indirekten Einfluss auf die Sicherheit der Primär-Assets (Daten). Auch die Sicherheit der Sekundär-Assets muss dementsprechend sichergestellt sein.

Abbildung A.4.2 zeigt Komponenten und Faktoren, die als Sekundär-Assets angesehen werden können und dementsprechend als potenzielle Angriffsziele ausgewählt werden können. Daten müssen sowohl in der zuvor beschriebenen zentralen Infrastruktur, auf dem Smartphone und auch während der Kommunikation geschützt werden. Dies ist über die Sekundär-Assets in Abbildung A.4.2

entsprechend abgebildet. Die in Abbildung A.4.2 gezeigte Hierarchie soll die Vielzahl an Sekundär-Assets andeuten, die im Zuge einer Sicherheitsüberprüfung einer Smartphone-Infrastruktur berücksichtigt werden müssen. Jede Komponente stellt ein mögliches Ziel eines Angriffs dar.

A.4.1.3 Sicherheitsrelevante Aspekte von Smartphones

Smartphones sind hochmobile Geräte, für die dementsprechend die gleichen bekannten Gefährdungen Gültigkeit haben, wie für klassische Endnutzergeräte wie bspw. PCs oder Notebooks. Dennoch unterscheiden sich Smartphones auf Grund ihrer Größe und ihrer Einsatzmöglichkeiten in folgenden Punkten von klassischen Geräten:

- Umgebung und Verwendung
- Potenzielle Vermischung von privater und geschäftlicher Verwendung
- Verwendung neuer und zusätzlicher Technologien
    - Positionsbestimmung via GPS, Mobilfunkzellen und WLAN
    - Integrierte Kameras
    - Vielfältige Kommunikationsmöglichkeiten über Mobilfunkstandards (GSM, UMTS (3G), LTE (4G), 5G), WLAN, Bluetooth, NFC, etc.
    - Umfangreiche Software
- Kombination unterschiedlicher Technologien
- Ausstattung mit zahlreichen Sensoren

A.4.1.4 Angriffsarten

Prinzipiell stehen einem Angreifer in Smartphone-basierten Infrastrukturen eine Vielzahl an Möglichkeiten zur Verfügung. Diese Methoden reichen vom Ausnützen von Sicherheitslücken in diversen Komponenten, über das Erlangen von physischem Zugriff auf sensible Daten, bis hin zu sozialen Angriffen, die direkt auf das Personal oder dessen soziales Umfeld abzielen.

- **Angriffe auf das Smartphone:** In diesem Fall ist das Smartphone selbst Ziel eines Angriffs, um auf das Smartphone selbst oder die Daten darauf Zugriff zu erlangen oder die Verwendung dieser einzuschränken.
- **Angriffe unter Verwendung des Smartphones:** Das Smartphone kann nicht nur direktes Ziel eines Angriffs sein, sondern auch für die Durchführung von Angriffen verwendet und missbraucht werden:

- **Spionage:** Sensoren wie Kameras oder Mikrofone ermöglichen es einem Angreifer unerlaubt Gespräche aufzuzeichnen oder kritische Daten zu fotografieren. Aufgrund ihrer Mobilität können Smartphones sehr leicht an kritischen Stellen positioniert werden und aufgezeichnete Daten an Dritte weiterleiten.
- **Angriffe auf das Netzwerk:** Smartphones mit entsprechender Software können verwendet werden, um Daten über Netzwerke zu sammeln. Bei schlechter Absicherung eines WLANs kann das Smartphone dazu benutzt werden weitere Informationen über das dahinterliegende Netzwerk zu sammeln und die Informationen für weitere Angriffe zu nutzen.

A.4.1.5 Gegenmaßnahmen

Im Gegensatz zur Flexibilität und Adapationsfähigkeit eines Angreifers sind Gegenmaßnahmen für Angriffe auf Smartphones bisher eher statischer Natur. Dabei kann im Prinzip zwischen zwei Kategorien unterschieden werden:

1. Technische Maßnahmen
2. Organisatorische Maßnahmen

Prinzipiell sind zur Wahrung der Sicherheit technische Maßnahmen zu bevorzugen, da sie ihre Sicherheitsfunktion ohne aktives Zutun einer Person immer gleich erfüllen. Die Wirksamkeit organisatorischer Maßnahmen hängt hingegen von vielen Komponenten ab. Sowohl bei technischen als auch bei organisatorischen Maßnahmen können Schwachstellen auftreten, die die Funktion der jeweiligen Sicherheitsmaßnahme einschränken, aufheben oder es Angreifern ermöglichen sie zu umgehen. Beispiele hierfür sind:

- Fehler in der Sicherheitsfunktion wie bspw. Verwendung eines unsicheren Verschlüsselungsalgorithmus
- Fehlende Sicherheitsfunktion wie bspw. Datenübertragung ohne Verschlüsselung
- Falsche Anwendung von Sicherheitsfunktionen wie bspw. die Wahl von zu einfachen Passwörtern
- Umgehen von Sicherheitsfunktionen
- Deaktivieren einer Sicherheitsfunktion wie bspw. das kurzfristige Verhindern der entfernten Datenlöschung auf einem gestohlenen Smartphone durch Deaktivieren der Internetverbindung

A.4.2 Bedrohungsanalyse

Dieser Abschnitt geht auf relevante Aspekte in der Durchführung einer Bedrohungsanalyse ein. Im Zuge einer solche Analyse müssen in jedem Fall die Besonderheiten von Smartphone-Infrastrukturen berücksichtigt werden. Eine umfassende Bedrohungsanalyse muss sowohl schützenswerte Daten (Primär-Assets) selbst, als auch Sekundär-Assets, die einen direkten oder indirekten Einfluss auf die Sicherheit von Primär-Assets haben, umfassen.

In diesem Abschnitt wird auf Assets, die sich in einer Smartphone-Infrastruktur üblicherweise ergeben, näher eingegangen und für diese allgemeine Bedrohungen skizziert. Damit kann dieser Abschnitt als Ausgangsbasis für eine eigene, detailliertere Bedrohungsanalyse dienen, in der dann auf die Spezifika der eigenen Infrastruktur gesondert eingegangen werden kann.

Die Gegenüberstellung von Asset und ihren Bedrohungen erfolgt in diesem Abschnitt über Identifikatoren. So werden Assets über Identifikatoren entsprechend dem Schema „A.x.y“ identifiziert, wobei x und y fortlaufende Zahlen sind. Die einem Asset A.x.y zuordenbaren Bedrohungen werden über den Identifikator B.x.y bezeichnet.

A.4.2.1 Daten

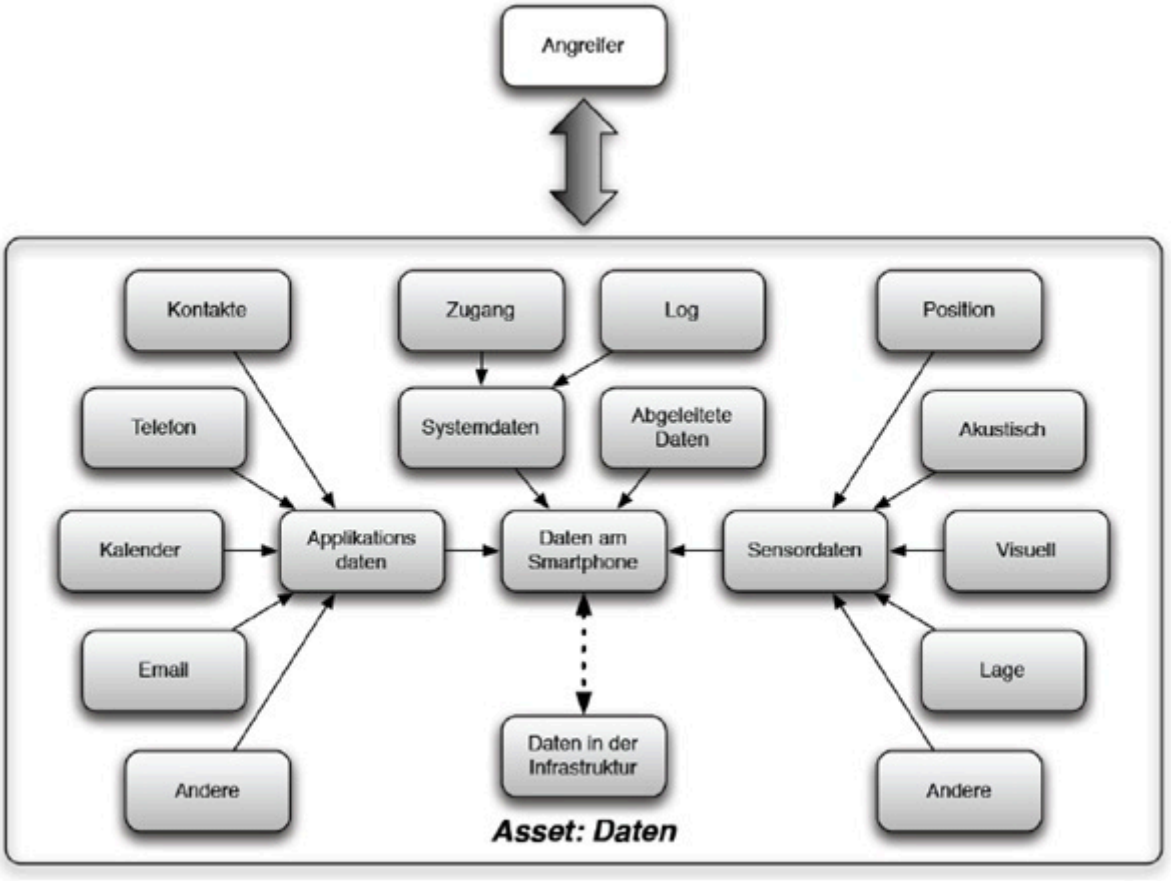

Abbildung A.4.3: Differenzierte Betrachtung des Kern-Assets: Daten

A1	**Daten**: Daten sind das Kern-Asset jeder Smartphone-Infrastruktur. Aufgrund der Vielfältigkeit der in einer Smartphone-Infrastruktur vorkommenden Daten wird zwischen folgenden Kategorien unterschieden: • Daten, die sich nur am Smartphone befinden, wie zum Beispiel persönliche Daten oder Eingaben der Benutzerin oder des Benutzers. • Daten der Smartphone-Sensoren, Systemdaten, etc. • Daten, die lokal am Smartphone gespeichert werden und eine Untermenge der Daten in der zentralen Infrastruktur darstellen. Dazu gehören u.a. E-Mails oder Daten, die über interne Services der Infrastruktur dem Smartphone zur Verfügung gestellt werden. Diese Daten spielen vor allem in Smartphone-basierten Unternehmensinfrastrukturen eine wichtige Rolle. • Daten, die gerade über einen Kommunikationskanal zwischen Smartphone und zentraler Infrastruktur transferiert werden. • Daten, die zum Beispiel im Zuge eines Prozessablaufs temporär verwendet werden. • Daten, die sich ausschließlich in der zentralen Infrastruktur befinden.
B1	**Zugriff auf Daten**: Ein Angreifer erhält unberechtigten Zugriff auf Daten der Smartphone-Infrastruktur. Mit Zugriff wird hier die Möglichkeit des Auslesens, Änderns oder Hinzufügens von Daten bezeichnet.

A1.1	**Applikationsdaten**: Dabei handelt es sich um Daten, die von Applikationen abgerufen oder erstellt werden. Der Begriff umfasst Daten von beliebigen Applikationen, unabhängig davon, ob diese für den Zugriff auf Unternehmensdaten oder im Rahmen der Verwendung des Smartphones für E-Government Applikationen eine Rolle spielen. Aufgrund des breiten Spektrums an Applikationsdaten werden einige spezielle Applikationsdaten im Folgenden noch exemplarisch als eigene Assets definiert.
B1.1	**Zugriff auf Applikationsdaten**: Applikationsdaten von E-Government Applikationen oder von Applikationen, die in einem Unternehmen verwendet werden, können für einen Angreifer von direktem Interesse sein oder als Basis für weitere Angriffe dienen.

A1.1.1	**Kontakte**: Diese Daten lassen unter anderem Rückschlüsse auf das geschäftliche und private soziale Umfeld der Benutzerin oder des Benutzers zu.
B1.1.1	**Zugriff auf Kontaktdaten**: Ein Angreifer kann Informationen über das soziale Umfeld der Benutzerin oder des Benutzers erhalten. Dadurch können Kontaktdaten von anderen Personen extrahiert werden, die unter Umständen für weitere Angriffe verwendet werden können. Ein Angreifer mit Hintergrundwissen über soziale Beziehungen kann dieses Wissen ausnutzen, um andere Personen im Namen einer Benutzerin oder eines Benutzers zu kontaktieren und somit Zugriff auf weitere Informationen und Dienste zu erhalten. Beispiele für derartige Informationen sind: • Private oder geschäftliche Beziehungen • Telefonnummern • E-Mail-Adressen

A1.1.2	**Telefondaten**: Dieser Begriff umfasst Daten, die mit der Telefonfunktionalität des Smartphones im Zusammenhang stehen. Dazu gehören unter anderem: • SMS-Nachrichten • Anruflisten • Gesprächsdaten von Telefongesprächen
B1.1.2	**Zugriff auf Telefondaten**: Ein Angreifer kann Zugriff auf Informationen in SMS-Nachrichten erhalten. Zusätzlich können anhand von Anruflisten Rückschlüsse über häufige Kontakte zu anderen Personen gezogen werden. Hierbei muss beachtet werden, dass Anruflisten im Allgemeinen getrennt von Kontaktdaten behandelt werden. Daher bewirkt das Löschen der Kontaktdaten typischerweise nicht das automatische Löschen der Anruflisten. Es können in diesem Fall zwar keine Namen mehr ausgelesen werden, die Telefonnummern der Kontakte in den Anruflisten stehen jedoch weiterhin zur Verfügung.

A1.1.3	**Kalender**: Hierbei handelt es sich um die Daten, die in Terminkalendern am Smartphone gespeichert werden.
B1.1.3	**Zugriff auf Kalenderdaten**: Ein Angreifer kann Informationen über den voraussichtlichen Aufenthaltsort von Benutzerinnen und Benutzern zu einem bestimmten Zeitpunkt erhalten. Zusätzlich können aus Kalenderdaten Informationen über das soziale Netzwerk des Benutzers bzw. der Benutzerin extrahiert werden.

A1.1.4	**Nachrichten von Messenger-Apps**: Verschiedene Messenger-Dienste werden nicht nur zur privaten, sondern oft auch zur geschäftlichen Kommunikation benutzt. Diese Nachrichten können daher sowohl sensible Daten privater Natur sowie kritische Informationen eines Unternehmens beinhalten.
B1.1.4	**Zugriff auf Messenger-Nachrichten**: Ein Angreifer kann Zugriff auf Nachrichten in Messenger-Apps erlangen und so deren Vertraulichkeit du auch Verfügbarkeit (durch Löschen) kompromittieren. Je nach Art der gespeicherten Daten können so auch unternehmensrelevante Informationen kompromittiert werden.

A1.1.5	**Push-Nachrichten**: Push-Nachrichten werden meist zur zeitnahen Information der Benutzerin oder des Benutzers über geänderte App-Inhalte (z.B. das Eintreffen einer neuen Nachricht) verwendet. Im Rahmen der Verwendung von multiplen Authentifizierungsfaktoren können Einmal-Codes auf diesem Wege an eine Begleit-App gesendet werden. Je nach gewählter Einstellung erfolgt die Darstellung des Nachrichteninhalts auch bei einem gesperrten Gerät.
B1.1.5	**Zugriff auf Push-Nachrichten**: Angreifer können Push-Nachrichten abfangen und so deren Inhalte kompromittieren. Werden über Push-Nachrichten sensible Daten wie z.B. Einmal-Codes übertragen, stellt dies ein besonderes Risiko dar.

A1.1.6	**E-Mail**: Dieses Asset umfasst alle E-Mails von Benutzerinnen und Benutzern, die für eine mobile Verwendung zur Verfügung stehen. Typischerweise wird ein Großteil der Kommunikation in einem Unternehmen via E-Mail durchgeführt. Daher kann davon ausgegangen werden, dass E-Mails kritische Informationen unterschiedlicher Natur enthalten und Rückschlüsse auf wichtige interne Zusammenhänge zulassen. Es handelt sich daher um ein sehr kritisches Asset innerhalb einer Unternehmensinfrastruktur. Für E-Government-Infrastrukturen ist dieses Asset dann von Bedeutung, wenn im Rahmen von E-Government-Diensten kritische Daten per E-Mail übertragen werden.
B1.1.6.a	**Zugriff auf kritische Daten in E-Mails**: Ein Angreifer kann Zugriff auf kritische Informationen, Dokumente oder andere Daten erhalten, die per E-Mail versendet werden. Beispiele für solche Daten sind: • **Persönliche Daten**: Dies umfasst jene Daten, die im Rahmen von E-Government Anwendungen verarbeitet oder übertragen werden. • **Finanzielle Daten eines Unternehmens**: Dazu gehören Bilanzen, Auftragsverrechnung, o.ä. • **Personaldaten**: Dies umfasst Adressdaten (und somit auch private Daten), Funktionen im Unternehmen, Gehaltslisten, etc. • **Daten über Aufträge**: Als Beispiel können hier finanzielle Details, Angebote oder Details zu aktuellen Vergaben genannt werden. • **Daten über Kunden oder Geschäftspartner**: Dazu gehören finanzielle Beziehungen, Aufträge, o.ä. • **Detaillierte Informationen über Produkte**: Die umfasst unter anderem Source-Codes oder interne Details, die aufgrund der Wettbewerbssituation nicht nach außen gelangen sollten. • **Daten über geplante kurzfristige und langfristige Entwicklungen im Unternehmen**: Dazu gehören Strategiepapiere, Personalpläne, Aufträge oder auch Kundenbeziehungen.
B1.1.6.b	**Zugriff auf Zugangsdaten**: Ein Angreifer kann Zugriff auf etwaige Zugangsdaten (z.B. zu webbasierten E-Government-Anwendungen) erhalten, die per E-Mail versendet wurden:

	• **Benutzernamen/Passwörter**: Oft werden Benutzernamen und Passwörter von diversen Zugängen per E-Mail versendet. Dies gilt sowohl für automatische Nachrichten von Konten, bei denen das Passwort vergessen wurde und die zurücksetzt werden sollen, als auch für das Weiterleiten von Zugangsdaten im Rahmen der Systemwartung. • **Rücksetzen von Konten**: Viele Dienste erlauben es, ein Konto über Informationen, die per E-Mail versendet werden, zurückzusetzen. Dabei kann prinzipiell zwischen zwei Verfahren unterschieden werden: ◦ *Senden von Passwörtern im Klartext*: In diesem Fall wird das Passwort eines Kontos im Klartext an die E- Mail Empfängerin oder den E-Mail-Empfänger übermittelt. Dabei können mehrere Probleme auftreten: - Wird ein E-Mail mit solchen Informationen archiviert, kann ein Angreifer unter Umständen das Passwort auslesen und somit Zugang zu dem Konto erhalten. - Da von der Benutzerin oder dem Benutzer oft dieselben Passwörter für mehrere Konten verwendet werden, kann ein Angreifer dadurch auf Zugriff zu anderen Konten der Benutzerin oder des Benutzers enthalten. ◦ *Senden von Informationen*: Vielfach werden URLs gesendet, die einmalig zum Zurücksetzen eines Kontos verwendet werden können. Hat ein Angreifer Zugang zu einem E-Mail-Konto kann er sich solche Rücksetz-E-Mails senden lassen, um damit Zugang zu anderen Konten zu erhalten.
B1.1.6.c	**Kommunikationsnetzwerk einer Person**: Ähnlich wie bei Kontaktdaten können durch Daten in E-Mails Informationen über das soziale Netzwerk von Benutzerinnen und Benutzern extrahiert werden. Dies umfasst sowohl private Aspekte wie Urlaub, Freizeit oder Freunde, als auch geschäftliche Angelegenheiten. Im Unterschied zu den Kontaktdaten befinden sich in E-Mails darüber hinaus noch eine Vielzahl weiterer Details, die einem Angreifer eine viel genauere Analyse der sozialen Beziehung von Benutzerinnen und Benutzern ermöglichen.
B1.1.6.d	**Funktion einer Person im Unternehmen**: Ein Angreifer kann anhand der Sender, Empfänger und Textinhalte feststellen, welche Aufgaben und Funktionen die Person innehat und wie sie in die Unternehmenshierarchie eingeordnet ist.

A1.1.7	**Daten sozialer Netzwerke**: Smartphones bieten Benutzerinnen und Benutzern diverse Möglichkeiten, um über eigene Applikationen mit sozialen Netzwerken zu kommunizieren. Diese Applikationen haben daher prinzipiell Zugriff auf sämtliche Informationen, die in diesem sozialen Netzwerk über die Benutzerin oder den Benutzer gespeichert sind.
B1.1.7	**Zugriff auf Daten sozialer Netzwerke**: Ein Angreifer kann über Applikationen zum Zugriff auf soziale Netzwerke verschiedenste persönliche Daten von Benutzerinnen und Benutzern extrahieren und so auf das soziale Umfeld rückschließen.

A1.1.8	**Navigationsdaten**: Auf Smartphones sind in der Regel Navigationsdaten gespeichert. Dies beinhaltet beispielsweise eine Liste von Orten, die die Benutzerin oder der Benutzer unter Verwendung von Navigationssoftware aufgesucht hat, oder die die Benutzerin oder der Benutzer regelmäßig aufsucht.
B1.1.8	**Zugriff auf Navigationsdaten**: Durch einen Zugriff auf Navigationsdaten kann ein Angreifer Rückschlüsse auf bereits besuchte oder regelmäßig aufgesuchte Aufenthaltsorte von Benutzerinnen und Benutzern ziehen.

A1.2	**Systemdaten**: Dabei handelt es sich um Daten, die vom System des Smartphones erstellt und für dessen Funktionalität benötigt werden. Beispiele dafür sind: • Logdateien, die für das Protokollieren von Ereignissen verwendet werden. Dazu gehören beispielsweise Listen aufgerufener Websites oder gestarteter Programme. Die verfügbaren Systemdaten hängen stark von der jeweiligen Smartphone-Plattform ab und können weite Bereiche abdecken. • Buffer, die Tastatureingaben oder andere Daten zwischenspeichern, um zum Beispiel eine Autokorrekturfunktion für Wörter anzubieten, die nicht in den mitgelieferten Wörterbüchern enthalten sind. • Schlüsselspeicher, die Zugangsdaten wie Benutzernamen und Passwörter speichern und von Applikationen für das automatische Einloggen bei verschiedenen Services verwendet werden.
B1.2.a	**Zugriff auf Zugangsdaten**: Kann ein Angreifer auf gespeicherte Anmeldedaten zugreifen, können diese unter Umständen für das Einloggen bei den entsprechend mitgespeicherten Services (z.B. E-Government-Dienste) verwendet werden. Beispiele für diese Bedrohung sind Angriffe auf Apples iOS-Keychain.
B1.2.b	**Zugriff auf Logs**: Diese Daten müssen unbedingt berücksichtigt werden, da sie unter Umständen einem Angreifer Seitenkanäle zu Informationen eröffnen, zu denen er sonst nicht direkt Zugriff hätte. Über Log-Daten erhält der Angreifer möglicherweise Zugriff auf Debug-Meldungen von Applikationen, die kritische Daten enthalten. E-Government Applikationen am Smartphone könnten bspw. benutzerbezogene Daten in Log-Dateien schreiben, auf die ein Angreifer dann Zugriff hätte.

A1.3	**Abgeleitete Daten**: Auch über abgeleitete Daten ist es möglich über Seitenkanäle Informationen zu sicherheitskritischen Daten zu erhalten. Da die Existenz möglicher Seitenkanäle von sehr vielen Faktoren abhängt, sollen hier nur einige Beispiele für mögliche Seitenkanäle auf Smartphone-Plattformen gegeben werden: • **Aufgerufene Websites**: Hat ein Angreifer keinen direkten Zugriff auf den Netzwerkverkehr des Smartphones, so gibt es unter Umständen Log-Dateien, die diese Daten enthalten. • **Positionen**: Ähnlich zum Verlauf besuchter Websites speichern diverse Navigationsapplikationen einen Verlauf besuchter Lokationen. Über diese Daten sind Rückschlüsse auf vergangene Aufenthaltsorte von Benutzerinnen und Benutzern möglich.
B1.3	**Zugriff auf abgeleitete Daten**: Kann ein Angreifer keinen direkten Zugriff auf die gewünschten Daten erhalten, so ist es ihm vielleicht möglich, indirekt über Seitenkanäle die gewünschten Informationen zu erhalten. Wenn ein Angreifer beispielsweise keinen direkten Zugriff auf die aktuelle Position der Benutzerin oder des Benutzers hat, kann er unter Umständen durch Auslesen der eindeutigen Identifikationsnummer der aktuellen Mobilfunkzelle und Abfragen von externen Datenbanken die Position feststellen.

A1.4	**Sensordaten**: Moderne Smartphones sind mit einer Vielzahl an Sensoren ausgestattet, die unter anderem die Aufzeichnung visueller und akustischer Daten oder eine exakte Positions- und Lagebestimmung des Geräts ermöglichen. Aufgrund der Vielzahl und Diversität an Informationen, die durch Sensoren gesammelt werden können, stellen diese ein besonders relevantes Asset dar. Auf Möglichkeiten einzelner Sensoren wird daher in Abschnitt A.4.2.4 dieses Anhangs näher eingegangen.

B1.4	**Zugriff auf Sensordaten**: Ein Angreifer kann auf Daten, die durch Sensoren aufgezeichnet und am Smartphone gespeichert wurden, zugreifen. Bedrohungen, die sich durch Zugriff auf verschiedene Sensordaten ergeben, werden in Abschnitt A.4.2.4 dieses Anhangs noch näher behandelt.

A.4.2.2 Plattformen

A2	**Smartphone-Plattform**: Die Smartphone-Plattform stellt Benutzerinnen und Benutzern die Grundfunktionalität zur Nutzung mobiler Dienste und Möglichkeiten zur Kommunikation mit der zentralen Infrastruktur zur Verfügung. Während die Hardware einer Smartphone-Plattform im Großen und Ganzen festgelegt ist und nur eingeschränkt erweitert werden kann, ist der Softwareumfang von Smartphones in der Regel flexibel erweiterbar und kann den jeweiligen Bedürfnissen von Benutzerinnen und Benutzern angepasst werden. Eine Smartphone-Plattform besteht im Allgemeinen aus den folgenden relevanten Komponenten: • **Hardware**: Dazu gehören unter anderem Touchscreen, Lautsprecher oder auch diverse Sensoren wie Mikrofon, GPS und Kompass. • **Betriebssystem**: Dieses stellt der Benutzerin oder dem Benutzer Grundfunktionalitäten wie Telefonie, Datenkommunikation und Softwareverwaltungsmechanismen zur Verfügung, kann aber darüber hinaus noch weitere Funktionen anbieten. • **Software**: Die Software von Smartphones kann in der Regel über sogenannte Apps flexibel erweitert werden. Diese werden in der Regel über zentrale App-Stores bereitgestellt und können von diesen bezogen werden. Für die sichere Verarbeitung von sicherheitskritischen Daten am mobilen Gerät sind die Integrität und Sicherheit dieser Komponenten eine zwingende Voraussetzung.
B2	**Kompromittierung der Smartphone-Plattform**: Gelingt es einem Angreifer eine oder mehrere Komponenten der Smartphone-Plattform zu kompromittieren, kann die Sicherheit der in der Smartphone-Infrastruktur gespeicherten und verarbeiteten Daten unter Umständen nicht mehr gewährleistet werden. Die Schwere der Bedrohung hängt dabei von der kompromittierten Komponente und der Art der sicherheitskritischen Daten ab.

A.4.2.3 Software

Die Software eines Smartphones ist im Gegensatz zu dessen Hardwarekonfiguration flexibel und einfach erweiterbar. Smartphone-Plattformen bieten Benutzerinnen und Benutzern in der Regel die Möglichkeit, zusätzliche Software-Module – sogenannte „Apps“ – über einen vordefinierten Installationsvorgang auf dem mobilen Gerät zu installieren. Trotz diverser Unterschiede zwischen verschiedenen Smartphone-Plattformen ist der prinzipielle Ablauf einer Softwareerweiterung meist ähnlich.
Die Benutzerin oder der Benutzer wählt die geeignete App aus verschiedenen zur Verfügung stehenden Quellen aus und installiert diese über einen vom Betriebssystem des Smartphones bereitgestellten Installationsmechanismus auf dem mobilen Gerät. Die Flexibilität der Softwareverwaltung von Smartphone-Plattformen bietet Angreifern verschiedene Möglichkeiten die Sicherheit der Plattform und damit der gesamten Smartphone-Infrastruktur zu kompromittieren.

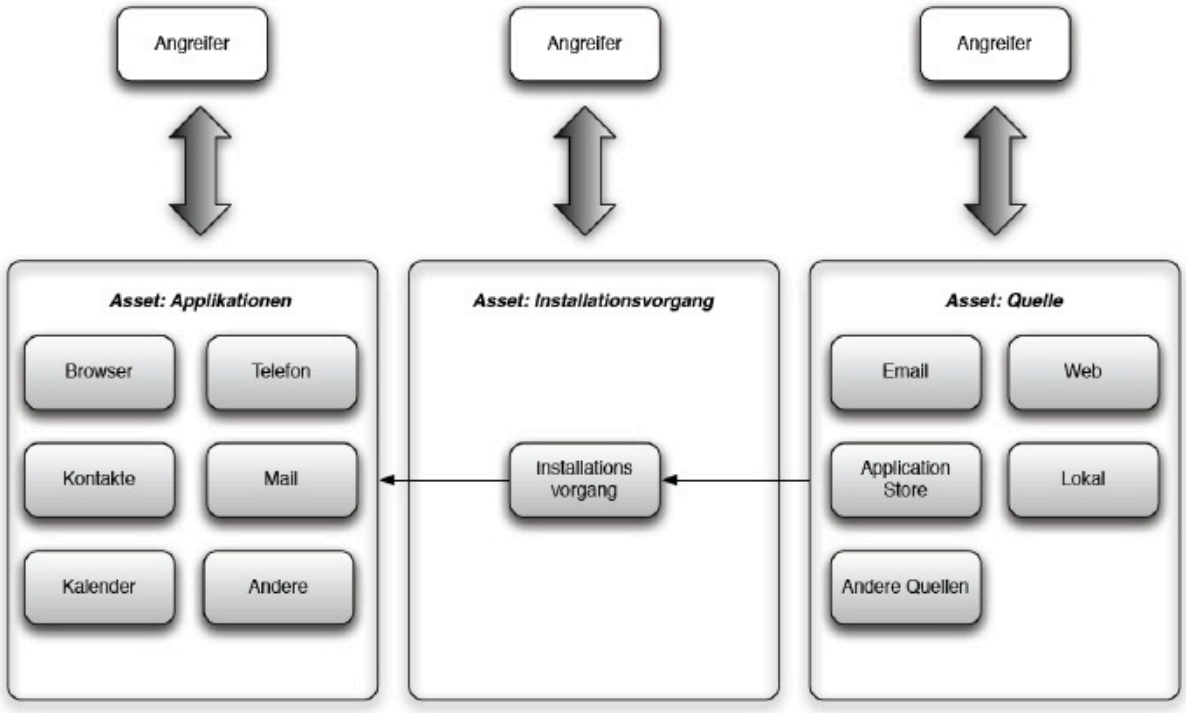

Abbildung A.4.4: Softwareverwaltung moderner Smartphone-Plattformen

A2.1	**Software**: Smartphones verfügen in der Regel über ein umfangreiches Softwareangebot und ein flexibles Softwaremanagementsystem, über das die Funktionalität des Geräts dynamisch erweitert und angepasst werden kann.
B2.1	**Kompromittierung der Software**: Funktionsreiche Softwarekomponenten und komplexe Softwaremanagementsysteme können eine Bedrohung für die Sicherheit von Smartphones und der auf ihnen gespeicherten Daten darstellen. Angreifer können die verschiedenen in Abbildung A.4.4 dargestellten Angriffspunkte nutzen, um das Gerät zu kompromittieren.

A2.1.1	**Applikationen (Apps)**: Applikationen sind eine Kernkomponente jeder Smartphone-Plattform. Durch Applikationen wird der Zugriff auf und die Verarbeitung von Daten ermöglicht. Da Applikationen potenziell Zugriff auf schützenswerte Daten am Smartphone haben, ist die Integrität und Sicherheit dieser Applikation von besonderer Relevanz.
B2.1.1.a	**Zugriff auf Daten über bestehende Applikationen (Apps)**: Angreifer können Zugriff auf bestehende Applikationen am Smartphone erlangen und diese für ihre Zwecke missbrauchen. Beispielsweise könnte eine Kamera-Applikation unbemerkt visuelle Daten der Umgebung aufnehmen, falls ein Angreifer Zugriff auf diese App hat. Dieses Angriffsszenario spielt vor allem in Unternehmensinfrastrukturen eine bedeutende Rolle. Generell sind folgende Angriffsszenarien denkbar: • Private oder geschäftliche Daten, die am Smartphone gespeichert sind, können extrahiert werden. • Funktionen des Smartphones wie zum Beispiel Sensoren können benutzt werden, um nicht gespeicherte Daten wie Position, Gespräche, visuelle Daten oder andere Sensordaten zu erhalten.

	Prinzipiell sind für derartige Angriffe alle Arten von Applikationen geeignet. Abhängig von der Funktionalität der App stehen dem Angreifer mehr oder weniger Möglichkeiten zur Verfügung, um Daten auszuspionieren. Von besonderem Interesse sind daher Applikationen, die einen möglichst umfangreichen Zugriff auf Daten und Funktionalitäten des Smartphones erlauben. Dazu gehören zum Beispiel: • **Sicherheitstools**: Speziell in offenen Märkten wie dem Android Market werden Sicherheitstools angeboten, die in unterschiedlichen Bereichen eingesetzt werden können. Dazu gehören die Durchführung von Port Scans in Netzwerken, das Aufspüren von WLAN Access Points, das Finden offener WLANs, die Analyse von Mobilfunkzellen und vieles mehr. Viele dieser Applikationen sammeln benutzerbezogene Applikationsdaten, die von einem Angreifer direkt oder indirekt für weitere Angriffe verwendet werden können. Zusätzlich existieren noch eine Reihe von Sicherheitstools, die Benutzerinnen und Benutzern unterschiedliche Features zur Absicherung des Smartphones – zum Beispiel im Falle des Diebstahls – bieten. Erlangt ein Angreifer Kontrolle über derartige Tools, können diese als Spionageprogramme verwendet werden. Je größer die Sicherheitsfunktionalität solcher Tools, desto besser können diese auch von Angreifern für deren Zwecke verwendet werden. • **Spionageapplikationen**: Viele Applikationen können Daten sammeln, die für einen Angreifer wertvoll sind. In vielen Fällen werben die Hersteller dieser Programme sogar damit, dass nach erfolgter Installation der Applikation deren Erkennen und Entfernen erschwert wird und zum Beispiel eine Fernsteuerung des Smartphones per SMS einfach möglich ist. Ein Zugriff auf diese Applikationen eröffnet einem Angreifer alle Möglichkeiten, die zum Verlust persönlicher oder kritischer Daten führen können. In diese Kategorie fallen prinzipiell auch die im vorherigen Punkte genannten Sicherheitstools, sofern diese von einem Angreifer für eigene Zwecke benutzt werden.
B2.1.1.b	**Zugriff auf Daten über Schadsoftware**: Applikationen, die von der Benutzerin oder dem Benutzer am Smartphone installiert werden, können mit Schadcode versehen sein. Dadurch ergeben sich prinzipiell dieselben Angriffsszenarien wie in B2.1.1.a. Da der Angreifer die Funktionalität der Schadsoftware jedoch selbst bestimmen kann und nicht auf die vorgegebene Funktionalität bereits installierter Apps limitiert ist, sind in diesem Szenario effizientere Angriffe möglich.

A2.1.2	**Installationsmechanismus**: Moderne Smartphone-Plattformen verfügen über einen Installationsmechanismus, über den von Benutzerinnen und Benutzern jederzeit zusätzliche Softwarekomponenten nachinstalliert werden können.
B2.1.2.a	**Einschleusen eigener Applikationen**: Durch Umgehung der Sicherheitsvorkehrungen des Installationsmechanismus kann es einem Angreifer gelingen, eigene Applikationen oder Schadsoftware auf einem Smartphone zu installieren.
B2.1.2.b	**Modifikation von zu installierenden Applikationen**: Durch Umgehung der Sicherheitsvorkehrungen des Installationsmechanismus kann ein Angreifer unter Umständen die zu installierenden Applikationen während des Installationsvorgangs seinen Anforderungen entsprechend modifizieren und auf diese Weise zum Beispiel Schadcode einschleusen.

A2.1.3	**Quelle**: Benutzerinnen und Benutzer können zusätzliche Softwarekomponenten von verschiedenen Quellen beziehen und über einen definierten Installationsmechanismus auf dem Smartphone installieren. Als Quelle kommen dabei beispielsweise Application-Stores oder das Web in Frage.

B2.1.3.a	**Einschleusen von Schadsoftware**: Angreifer können unzureichend geschützte Quellen verwenden, um eigene Schadsoftware einzubringen. Ist die Schadsoftware als solche nicht zu erkennen, kann sie über den vorgesehenen Installationsmechanismus den Weg auf Smartphones finden.
B2.1.3.b	**Verändern bestehender Applikationen**: Sind Quellen, in denen Applikationen zentral gespeichert werden, nicht ausreichend geschützt, können Angreifer bestehende Applikationen modifizieren und mit Schadcode versehen.

A.4.2.4 Sensoren

Sensoren stellen für Smartphones ein wichtiges Instrument dar, welches die Implementierung funktionsreicher Applikationen wie zum Beispiel von Navigationssystemen erlauben. Durch die Möglichkeit Informationen aus der unmittelbaren Umgebung des Smartphones aufzuzeichnen und detaillierte Lage- und Positionsbestimmungen durchzuführen, stellen Sensoren jedoch auch für Angreifer ein attraktives Ziel dar.

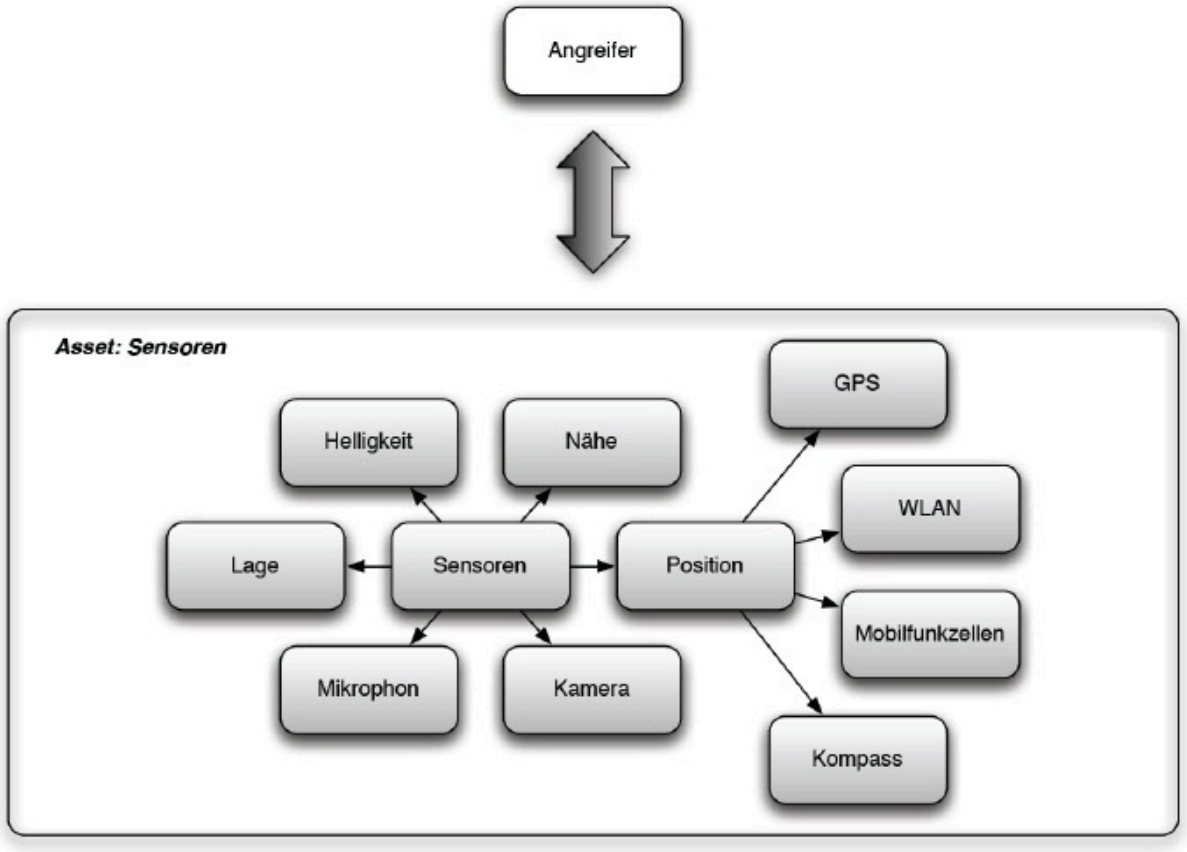

Abbildung A.4.5: Arten von Sensoren

A2.2	**Sensoren**: Smartphones sind mit einer Reihe von Sensoren ausgestattet, die Rückschlüsse auf die Umgebung des Geräts zulassen. Dazu gehören unter anderem Kameras, Navigationssysteme, Kompasse, sowie Helligkeits-, Lage- und Annäherungssensoren.

B2.2	**Zugriff auf Sensordaten**: Bekommt ein Angreifer Zugriff auf Sensoren oder die von diesen Sensoren aufgezeichneten Daten, können diese kompromittiert oder als Basis für weitere Angriffe verwendet werden.

A2.2.1	**Positionsdaten**: Damit werden alle Daten bezeichnet, die für die Positionsbestimmung der Benutzerin oder des Benutzers verwendet werden können. In erster Linie handelt es sich hierbei um Positionsangaben die anhand von WLANs, Mobilfunknetzwerken oder direkt über Navigationssysteme wie GPS, Glonass, Galileo oder Beidou bezogen werden. Es müssen jedoch auch Daten berücksichtigt werden, die eine indirekte Ableitung der Position ermöglichen. Dies kann beispielsweise über MAC Adressen von WLAN Access Points, Identifikationsnummern von Mobilfunkzellen oder textuelle Positionsangaben wie Ortsnamen erfolgen.
B2.2.1	**Zugriff auf Positionsdaten**: Ein Angreifer kann entweder auf gespeicherte Positionsdaten am Smartphone oder direkt auf die Positionssensoren des Geräts zugreifen, um Informationen über die aktuelle Position der Benutzerin oder des Benutzers zu erhalten. Diese Informationen können als Basis für weitere Angriffe verwendet werden. Auf folgende Informationen könnte so beispielsweise indirekt rückgeschlossen werden: • Tagesabläufe der Benutzerin oder des Benutzers • An-/Abwesenheit der Benutzerin oder des Benutzers an bestimmten Orten • Lokationen, die für die Benutzerin oder den Benutzers relevant sind • Daten über das soziale Netzwerk der Benutzerin oder des Benutzers und über geschäftliche oder private Beziehungen

A2.2.2	**Akustische Daten**: Hierbei handelt es sich um Audiodaten, die sich entweder auf dem Speicher des Smartphones befinden oder direkt über das Mikrofon zur Verfügung stehen.
B2.2.2	**Zugriff auf akustische Daten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf gespeicherte akustische Daten oder direkt auf das Mikrofon bekommen. Dadurch kann der Angreifer zum Beispiel Zugriff auf folgende Daten erlangen: • Aufzeichnen von vertraulichen Gesprächen • Aufzeichnen von Telefongesprächen der Benutzerin oder des Benutzers • Aufzeichnen von Sprachnachrichten der Benutzerin oder des Benutzers

A2.2.3	**Visuelle Daten**: Hierbei handelt es sich um Bild- oder Videodaten, die entweder auf dem Speicher des Smartphones liegen, oder direkt über die Kamera zur Verfügung stehen.
B2.2.3	**Zugriff auf visuelle Daten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf gespeicherte visuelle Daten oder direkten Zugriff auf die Kamera erlangen. Im Gegensatz zum Mikrofon ist hier aufgrund der Notwendigkeit der Positionierung des Smartphones die Wahrscheinlichkeit geringer, dass gewünschte Informationen gezielt aufgezeichnet werden können. Durch Zugriff auf am Smartphone verfügbare visuelle Daten kann ein Angreifer zum Beispiel Zugriff auf folgende Informationen erlangen: • Erstellen von Videos/Fotos von kritischen Daten (z.B. Dokumente) • Erkennen von Sicherheitsmaßnahmen innerhalb eines Unternehmens oder einer Behörde

	• Erkennen von anderen Merkmalen wie Personen, Objekte oder Zugangscodes, die als Basis für weitere Angriffe dienen können.

A2.2.4	**Helligkeitsdaten**: Helligkeitssensoren erlauben modernen Smartphones die Feststellung der Helligkeit der aktuellen Umgebung.
B2.2.4	**Zugriff auf Helligkeitsdaten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Helligkeitsdaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

A2.2.5	**Lagedaten**: Lagesensoren erlauben modernen Smartphones die Feststellung der aktuellen Lage des Smartphones im Raum.
B2.2.5	**Zugriff auf Lagedaten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Lagedaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

A2.2.6	**Annäherungsdaten**: Annäherungssensoren erlauben modernen Smartphones die Feststellung von Objekten in der Nähe des Geräts. Dies wird hauptsächlich dazu verwendet, um während eines Telefonats das Display des Smartphones automatisch auszuschalten.
B2.2.6	**Zugriff auf Annäherungsdaten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Annäherungsdaten erlangen. Dadurch ist es ihm beispielsweise möglich, auf Anzahl und Dauer von Telefonaten rückzuschließen, falls diese Information auf direktem Weg nicht zugänglich ist.

A2.2.7	**Beschleunigungsdaten**: Beschleunigungssensoren erlauben modernen Smartphones die Messung der aktuellen Beschleunigung des Geräts.
B2.2.7	**Zugriff auf Beschleunigungsdaten**: Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Beschleunigungsdaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

A.4.2.5 Kommunikation

Im Zusammenhang mit dem Schutz sicherheitskritischer Daten einer Smartphone-Infrastruktur spielt die Kommunikation zwischen den einzelnen Komponenten der Infrastruktur eine zentrale Rolle.

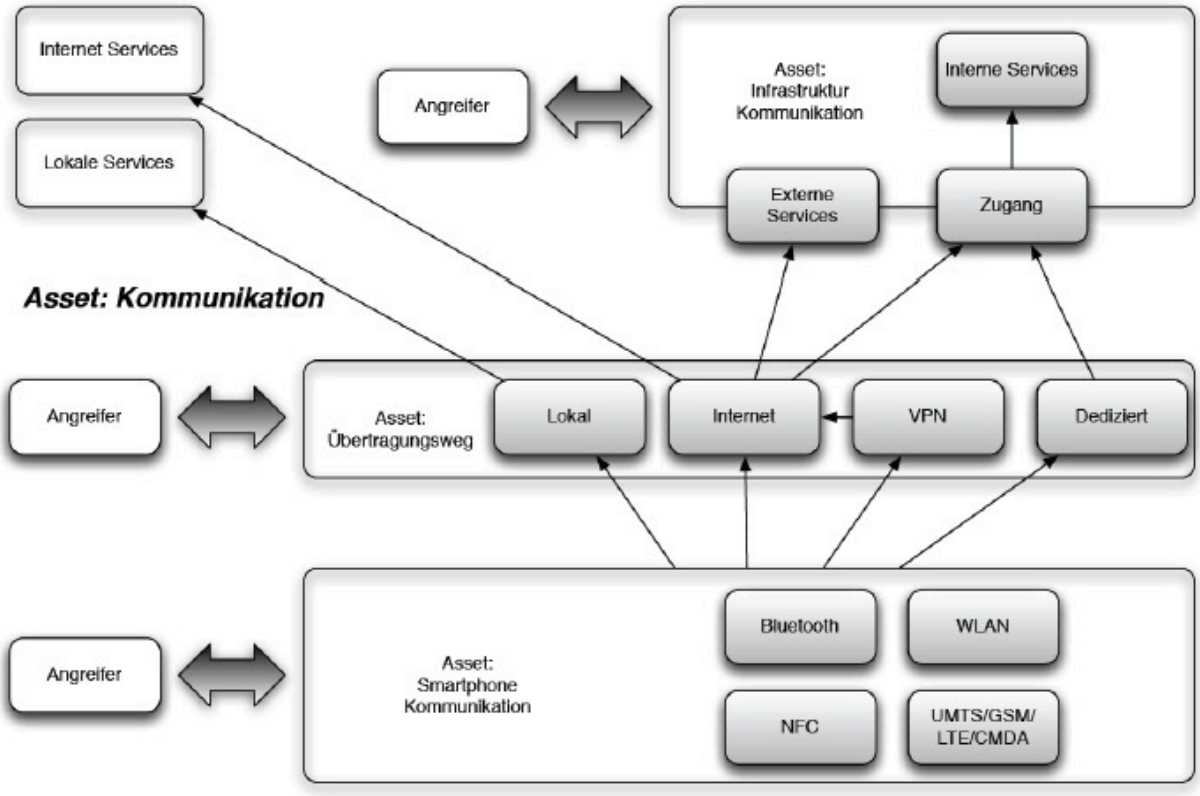

Abbildung A.4.6: Kommunikationspfade innerhalb einer Smartphone-Infrastruktur

Das Asset „Kommunikation“ kann generell in drei den einzelnen Bereichen einer Smartphone-Infrastruktur entsprechenden Assets unterteilt werden. Sämtliche für die Kommunikation verantwortliche Komponenten der Smartphone-Plattform werden im Asset „Smartphone Kommunikation“ zusammengefasst. Relevante Kommunikationskomponenten der zentralen Infrastruktur werden hingegen durch das Asset „Infrastruktur Kommunikation“ abgedeckt. Neben diesen beiden Assets gibt es noch das Asset „Übertragungsweg“, welches Aspekte des Kommunikationspfades zwischen zentraler Infrastruktur und Smartphone-Plattform abdeckt.

A3	**Kommunikation**: Dieses Asset betrifft einerseits die Kommunikation zwischen der Smartphone- Plattform und der zentralen Infrastruktur eines Unternehmens oder einer Behörde, andererseits aber auch die Kommunikation der Smartphone-Plattform mit anderen externen Komponenten. Dabei kommen unterschiedliche im Folgenden näher analysierte Kommunikationskanäle und Interfaces zum Einsatz.
B3	**Angriffe auf die Kommunikation**: Erhält ein Angreifer Zugriff auf einen Kommunikationskanal, so hat er unter Umständen auch auf übermittelte Daten lesend und/oder schreibend Zugriff. Dadurch ergeben sich unterschiedliche Bedrohungen, deren Details von den jeweiligen unterschiedlichen Subkomponenten abhängen.

A3.1	**Smartphone-Kommunikation**: Smartphones verfügen über diverse Kommunikationsmöglichkeiten, die einen Datenaustausch mit zentralen Infrastrukturen, externen Komponenten oder auch anderen Smartphones erlauben.
B3.1	**Angriffe auf die Smartphone-Kommunikation**: Aufgrund der Exponiertheit von Smartphones und der meist kabellosen Übertragungstechniken, ergeben sich für die Smartphone-Kommunikation zahlreiche Angriffsmöglichkeiten und Gefahren. Gelingt es einem Angreifer die Kommunikation zu kompromittieren, können übermittelte und potenziell sicherheitskritische oder persönliche Daten gestohlen werden.

A3.1.1	**WLAN**: WLANs werden vor allem dann verwendet, wenn kein Zugriff auf ein Mobilfunkdatennetzwerk besteht. In diesen Fällen ermöglichen WLANs den Zugang zum Internet und erlauben Zugriff auf Ressourcen und Daten der zentralen Infrastruktur. WLANs werden auch bevorzugt verwendet, um die Datenübertragung über Mobilfunkdatennetze zu minimieren, da für diese oft Limits bestehen. In der Regel stellt der Internetzugriff via WLAN oft die präferierte Variante dar, während Mobilfunkdatennetze dann zum Einsatz kommen, wenn kein verwendbares WLAN zur Verfügung steht.
B3.1.1	**Angriffe auf WLANs**: Vor allem für öffentliche WLANs ergeben sich vielseitige Bedrohungen. Diese Bedrohungen sind prinzipiell seit Einführung dieser Technologie bekannt, gewannen jedoch mit der weiten Verbreitung von WLANs zunehmend an Bedeutung. Folgende Angriffsszenarien kompromittieren die Sicherheit von WLANs: • **Nicht vertrauenswürdige WLANs**: WLAN-Hotspots können sehr einfach in Betrieb genommen werden und sind prinzipiell an allen Orten einsetzbar. Mobile Geräte können sehr einfach als Ad-Hoc Access Point konfiguriert werden. Auch Smartphones können so beispielsweise als WLAN-Hotspot betrieben werden. Generell gilt, dass WLANs nur eingeschränkt vertraut werden kann, da diese auch von Angreifern betrieben werden können. • **Auslesen übertragener Daten**: Bei WLANs, die Dienste ohne weitere Schutzmechanismen wie WPA anbieten, hat ein Angreifer, der sich in der Empfangs- und Sendereichweite des WLANs befindet, die Möglichkeiten Zugriff auf alle im WLAN übermittelten Daten zu erhalten. Dies betrifft einen Großteil aller WLANs, da Schutzmechanismen wie WPA bei Hotspots typischerweise durch nachgelagerte Authentifizierungsmaßnahmen ersetzt werden. Demzufolge müssen folgende Implikationen für Daten beachtet werden: ◦ *Unverschlüsselte Daten* wie jene, die über die Protokolle HTTP oder DNS übertragen werden, sind von einem Angreifer einsehbar und manipulierbar. Einem Angreifer stehen daher viele Methoden zur Verfügung, die verschiedene Arten von Angriffen ermöglichen. Diverse Phishing-Angriffe ermöglichen bspw. das Fälschen von DNS-Einträgen, etc. Ungeschützt übertragene Informationen werden dem Angreifer im Klartext zugänglich gemacht und erlauben ihm übertragene Daten während des Transfers zu manipulieren. Dadurch kann bspw. Schadsoftware in den nicht geschützten Transfer von Daten eingefügt werden. ◦ *Verschlüsselte Daten*, die bspw. über HTTPS gesichert sind für Man-in-the-middle-Angriffe anfällig. Ein Angreifer kann etwa ein Zertifikat einer HTTPS Verbindung fälschen. Außerdem muss berücksichtigt werden, dass Applikationen die über HTTPS Kommunizieren, nur dann sicher sind, wenn auch die eingesetzten Zertifikate von der Applikation verlässlich geprüft werden.

A3.1.2	**UMTS/GSM/LTE/CDMA/5G**: Datenverbindungen können auch über Mobilfunktechnologien wie GSM, UMTS, LTE, CDMA oder 5G hergestellt werden.
B3.1.2	**Angriffe auf UMTS/GSM/LTE/CDMA/5G**: Hier werden keine spezifischen Bedrohungen genannt. Die Unsicherheit von GSM-Netzen ist bekannt, spielt aber weiterhin keine entscheidende Rolle. Für die Übertragung von Daten über das Internet muss ohnehin davon ausgegangen werden, dass die verwendeten Netzwerke nicht vertrauenswürdig sind.

A3.1.3	**Bluetooth**: Bluetooth kommt hauptsächlich zur Anbindung externer Geräte oder zur Verbindung mit anderen Smartphones zur Anwendung.
B3.1.3	**Angriffe auf Bluetooth**: Gelingt es einem Angreifer die Bluetooth-Kommunikation zu kompromittieren, kann er Zugriff auf die über diese Schnittstelle übertragenen Daten erhalten.

A3.1.4	**NFC**: NFC basiert auf der RFID Technologie und ermöglicht sowohl das Auslesen passiver RFID- Tags mit Smartphones als auch eine RFID-basierte Kommunikation zwischen Smartphones.
B3.1.4	**Angriffe auf NFC**: Gelingt es einem Angreifer die NFC-Kommunikation zu kompromittieren, kann er Zugriff auf die über diese Schnittstelle übertragenen Daten erhalten.

A3.2	**Übertragungsweg**: Als Übertragungsweg bezeichnet man die Strecke zwischen dem Smartphone und dem jeweiligen Kommunikationspartner. Als Kommunikationspartner kann beispielsweise eine zentrale Infrastruktur oder auch ein anderes Smartphone fungieren.
B3.2	**Angriffe auf den Übertragungsweg**: Sind Daten am Übertragungsweg nicht geeignet gesichert, können diese von einem Angreifer kompromittiert werden. Je nach Übertragungsweg ergeben sich dabei unterschiedliche Gefahrenpotenziale.

A3.2.1	**Übertragungsweg zu lokalen Services**: Darunter versteht man den Kommunikationspfad zu Services, die in der lokalen Umgebung des Smartphones zur Verfügung stehen. Diese können von einfachen Bluetooth-Freisprecheinrichtungen, über den direkten Datenaustausch mit anderen Smartphones via Bluetooth oder WLAN bis zu von der lokalen Infrastruktur angebotenen Intranet Services reichen.
B3.2.1	**Angriffe auf den Kommunikationspfad zu lokalen Services**: Für den Zugriff auf lokale Services kommen üblicherweise Bluetooth und lokale Netzwerkverbindungen (WLAN) zur Anwendung. Es gelten hier also alle Bedrohungen, die auch bei diesen Services auftreten. In diesem Zusammenhang besonders relevant sind die Bedrohungsszenarien B3.1.1 und B3.1.3. Inkludieren diese Übertragungswege auch weitere öffentliche Netzwerke, so muss auch das Bedrohungsszenario B3.2.3.a speziell beachtet werden.

A3.2.2	**Dedizierte Übertragungswege**: Hierbei handelt es sich um potenziell proprietäre Kommunikationsverbindungen, die zwischen den Smartphones und der zentralen Infrastruktur zur Verfügung gestellt werden. Die Verbindungen können dabei sowohl auf privaten als auch auf öffentlichen Netzwerken aufbauen.
B3.2.2	**Angriffe auf dedizierte Übertragungswege**: Mögliche Angriffe hängen von der jeweiligen Implementierung des dedizierten Übertragungsweges ab. Aus diesem Grund ist eine differenzierte Betrachtung der eingesetzten Protokolle nötig.

A3.2.3	**Internet**: Bei diesem Übertragungsweg werden Daten über öffentliche Netzwerke transportiert. Dies ist in der Regel der am häufigsten gebrauchte Übertragungsweg, sofern keine dedizierten Übertragungswege zur Verfügung stehen.
B3.2.3.a	**Angriffe auf öffentliche Netzwerke**: Generell gelten hier alle Bedrohungen und Probleme, die mit dem Transport von Daten über öffentliche Netzwerke verbunden sind. Ein Angreifer kann Zugriff auf nicht verschlüsselte Daten erhalten und diese auslesen oder manipulieren. Ein direkter Angriff auf diese öffentlichen Netzwerke ist für einen Angreifer mit großem Aufwand verbunden, da er typischerweise keinen Zugriff auf die Komponenten dieser Netzwerke hat. Diese Bedrohung spielt daher vor allem in Szenarien, in denen Angreifer mit sehr großen Ressourcen oder Kontrolle über diese Netzwerke im Spiel sind, eine große Rolle.
B3.2.3.b	**Zugang zum Internet**: Um Zugriff auf das Internet zu bekommen werden entsprechende Zugangspunkte benötigt. Speziell die weite Verbreitung von WLANs bietet einem Angreifer in diesem Zusammenhang viele Möglichkeiten Zugriff auf Daten zu erhalten. In diesem Zusammenhang wird wiederum auf Bedrohungsszenario B3.1.1 verwiesen.

A3.2.4	**VPN-Verbindungen**: VPN-Verbindungen dienen dem sicheren Zugriff auf die zentrale Infrastruktur eines Unternehmens. Im Rahmen von E-Government Diensten spielen diese Verbindungen daher eine untergeordnete Rolle. Über eine VPN-Verbindung wird im Prinzip die geschützte Umgebung einer zentralen Infrastruktur auf das mobile Smartphone ausgedehnt. Sämtliche Kommunikation zwischen Smartphone-Plattform und zentraler Infrastruktur wird über Secure Messaging abgesichert. VPN-Verbindungen bauen dabei in der Regel auf öffentlichen Netzwerken wie dem Internet auf. Da der erfolgreiche Aufbau einer VPN-Verbindung einen Zugang zu internen Services der zentralen Infrastruktur ermöglicht, muss eine VPN-Verbindung selbst als Asset betrachtet werden. Im Besonderen gilt dies für Berechtigungsnachweise wie Passwörter, kryptographische Schlüssel und Zertifikate, die auf dem Smartphone gespeichert sind und für den Aufbau einer VPN-Verbindung benötigt werden.
B3.2.4	**Angriffe auf VPN-Verbindungen**: Gelingt es einem Angreifer eine VPN-Verbindung zur zentralen Infrastruktur aufzubauen, kann dieser unter Umständen Zugriff auf interne Services und Ressourcen eines Unternehmens erlangen. Berechtigungsnachweise, die für den Aufbau einer VPN-Verbindung erforderlich sind, müssen daher sicher verwahrt und dürfen für einen Angreifer nicht zugänglich sein.

A3.3	**Infrastruktur-Kommunikation**: Die Infrastruktur-Kommunikation umfasst jene Komponenten, die für eine Kommunikation mit externen Smartphones verantwortlich sind. Dazu gehören beispielsweise zentrale Zugangspunkte oder externe Services.

B3.3	**Zugriff auf die Infrastruktur-Kommunikation**: Erhält ein Angreifer Zugriff auf diese Komponenten, kann er über diese unter Umständen auf Daten innerhalb der zentralen Infrastruktur zugreifen.

A3.3.1	**Externe Services**: Externe Services werden in der Regel verwendet, um ausgewählte Daten aufzubereiten und zu repräsentieren. Beispiele für solche Services sind etwa Webauftritte von Behörden im Rahmen von E-Government-Diensten oder Services zur Kommunikation mit Partnerunternehmen. Diese Services stehen in keinem ausschließlichen Zusammenhang mit Smartphones, können über diese jedoch meist auch genutzt werden. Da externe Services potenziell ebenfalls Zugriff auf interne Daten bzw. ein Subset davon haben, ist deren Sicherheit von Bedeutung.
B3.3.1	**Zugriff auf externe Services**: Durch das Ausnützen von Sicherheitslücken in externen Services kann ein Angreifer Zugriff auf kritische Daten der zentralen Infrastruktur bekommen.

A3.3.2	**Zugang**: Über einen definierten Zugang können externe Geräte wie Smartphones in die zentrale Infrastruktur eingebunden werden und Zugriff auf interne Services erlangen. In den meisten Fällen wird es sich bei diesem Zugang um einen VPN-Endpunkt handeln, theoretisch sind aber auch andere Ansätze denkbar. Diese Komponente spielt vor allem in Unternehmensinfrastrukturen eine wichtige Rolle.
B3.3.2.a	**Kompromittierung des Zugangs**: Gelingt es einem Angreifer die Sicherheitsmechanismen des Zugangs zu umgehen, kann über diesen Zugang Zugriff auf interne Services und damit auf interne Daten der zentralen Infrastruktur erlangt werden.
B3.3.2.b	**Missbräuchliche Verwendung eines Smartphones**: Erhält ein Angreifer Zugang zu einem Smartphone, auf dem eine aufrechte Verbindung zur zentralen Infrastruktur besteht und benötigte Berechtigungsausweise gespeichert sind, kann er Zugriff auf interne Services und damit auf Daten der zentralen Infrastruktur erlangen.

A.4.2.6 Zentrale Infrastruktur

Die zentrale Infrastruktur stellt neben der Smartphone-Plattform und dem Kommunikationsweg zwischen Infrastruktur und Smartphone-Plattform den dritten relevanten Bereich einer Smartphone-Infrastruktur dar. Die zentrale Infrastruktur wird prinzipiell der geschützten Umgebung zugeordnet. Durch den Einsatz von Smartphones können jedoch auch für die in der Infrastruktur gespeicherten und verarbeiteten Daten zusätzliche Bedrohungen entstehen. Die in diesem Abschnitt angestellten Überlegungen betreffen speziell Smartphone-basierte Unternehmensinfrastrukturen.

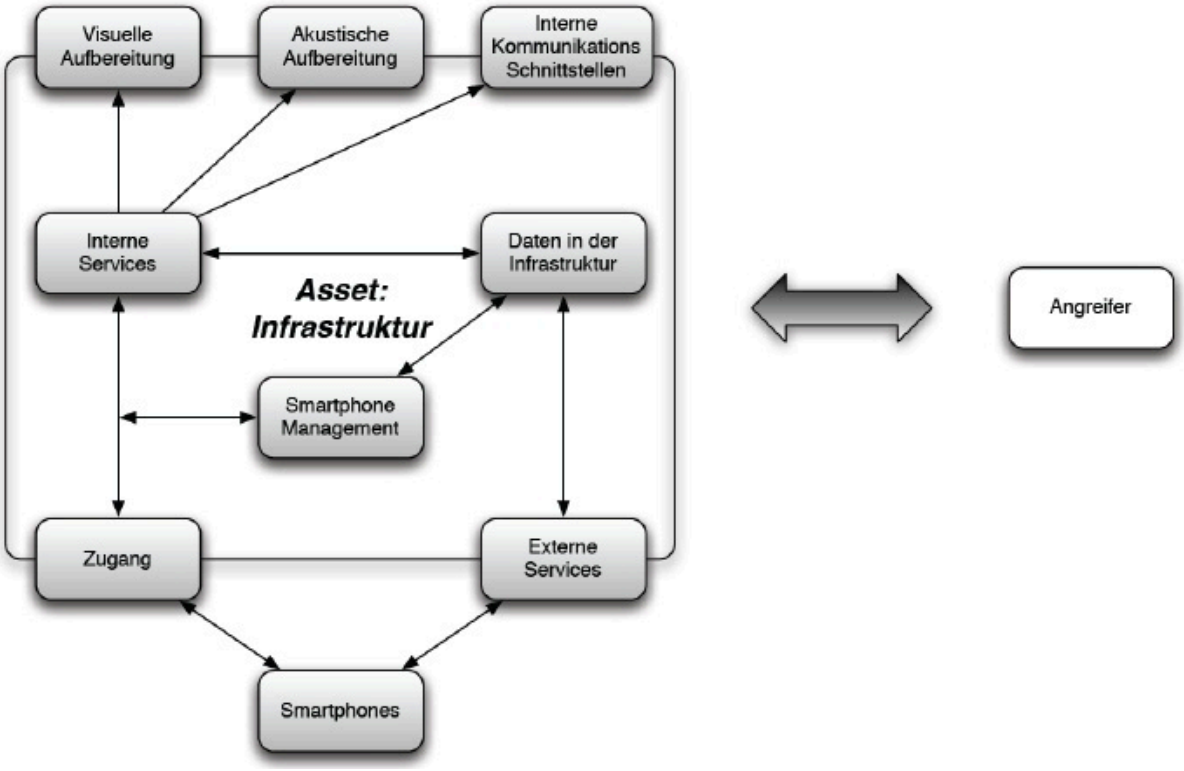

Abbildung A.4.7: Relevante Komponenten der zentralen Infrastruktur

A4	**Zentrale Infrastruktur**: Die zentrale Infrastruktur enthält in der Regel diverse Komponenten, die durch den Einsatz von Smartphones gefährdet werden können.
B4	**Zugriff auf Komponenten der zentralen Infrastruktur**: Durch unerlaubten Zugriff auf einzelne Komponenten der zentralen Infrastruktur können die in der Infrastruktur gespeicherten und verarbeiteten Daten kompromittiert werden.

A4.1	**Interne Services**: Hierbei handelt es sich um interne Services, die nicht vom Internet aus zugänglich sind. Dies können beispielsweise E-Mail-Dienste oder andere Services sein, die ausschließlich im Intranet eines Unternehmens zur Verfügung stehen. Diese Services sind prinzipiell nicht Bestandteil dieser Analyse, es wird aber davon ausgegangen, dass diese Services den Zugriff auf kritische Informationen ermöglichen würden.
B4.1	**Zugriff auf interne Services**: Erhält ein Angreifer Zugriff auf interne Services, kann er damit Zugriff auf interne Daten der zentralen Infrastruktur erlangen. Für E-Government Infrastrukturen spielt diese Bedrohung eine untergeordnete Bedeutung, da Benutzerinnen und Benutzer in der Regel über keinen VPN-Zugang zu internen E-Government Services verfügen.

A4.2	**Visuelle Aufbereitung**: Zusätzlich zu internen und externen Services, die den Zugriff auf Daten ermöglichen, werden interne Daten von Behörden oder Unternehmen intern oft visuell aufbereitet. Bei der visuellen Aufbereitung handelt es sich neben der elektronischen Aufbereitung auf Bildschirmen zum größten Teil um das Ausdrucken von Dokumenten.

B4.2.a	**Aufzeichnen von visuellen Informationen mit einem Smartphone, das im Besitz des Angreifers ist**: Ein Angreifer, der visuellen Zugriff auf die Infrastrukturkomponenten des Unternehmens hat, kann sein Smartphone benutzen, um visuelle Informationen in Form von Videos oder Fotos aufzuzeichnen. Diese Informationen können je nach Beschaffenheit des Unternehmens und der verfügbaren Informationen sehr unterschiedlicher Natur sein. Beispiele für Informationen, die durch das Erstellen von Fotos oder Videos kompromittiert werden können, sind: • Kritische oder persönliche Informationen auf Bildschirmen • Zugangsdaten wie Eingaben auf PIN-Pads, Tastaturen und anderen Eingabegeräten • Ausgedruckte Dokumente, die kritische oder persönliche Informationen beinhalten • Sicherheitsfunktionen wie Schließsysteme, Wachpersonal oder andere Vorkehrungen
B4.2.b	**Aufzeichnen von visuellen Informationen mit einem Smartphone, das ein Angreifer mit Schadsoftware infiziert hat**: Diese Bedrohung ist ähnlich zur Bedrohung B4.2.a. Allerdings wird hier davon ausgegangen, dass der Angreifer keinen persönlichen Zugriff auf visuelle Informationen hat, sondern ein Smartphone einer Benutzerin oder eines Benutzers mit Schadsoftware infiziert hat, die ihm einen Zugriff auf die Kamera oder Daten der Kamera erlaubt. Prinzipiell können dabei die gleichen visuellen Informationen wie im Bedrohungsszenario B4.2.a kompromittiert werden. Allerdings ist aufgrund der Tatsache, dass der Angreifer das Smartphone nicht selbst ausrichten kann, die Wahrscheinlichkeit, Zugriff auf relevante Informationen zu bekommen, bedeutend geringer. Anmerkung: Bei Bedrohungsszenarien für akustische Daten ist das Bedrohungspotenzial genau umgekehrt.

A4.3	**Akustische Aufbereitung**: Darunter versteht man die akustische Wiedergabe von Daten etwa in Form von persönlichen Gesprächen oder mündlichen Präsentationen.
B4.3.a	**Aufzeichnen von akustischen Informationen mit einem Smartphone, das im Besitz des Angreifers ist**: Ein Angreifer, der mit seinem Smartphone in der Reichweite von vertraulichen Gesprächen ist, kann das Gerät benutzen, um diese Gespräche aufzuzeichnen. Diese Informationen können je nach Beschaffenheit des Unternehmens oder der Behörde sehr unterschiedlicher Natur sein und prinzipiell ein breites Spektrum an relevanten Informationen umfassen. Beispiele für derartige akustische Informationen sind etwa: • Gespräche zwischen Mitarbeiterinnen und Mitarbeitern des Unternehmens oder der Behörde, bei denen kritische Informationen diskutiert werden • Gespräche, die in Meetings geführt werden • Alle anderen Informationen, die im Rahmen von persönlichen Gesprächen behandelt werden
B4.3.b	**Aufzeichnen von akustischen Informationen mit einem Smartphone, das ein Angreifer mit Schadsoftware infiziert hat**: Diese Bedrohung ist ähnlich zur Bedrohung B4.3.a. Allerdings geht man hier davon aus, dass der Angreifer keinen persönlichen Zugriff auf akustische Informationen hat, sondern ein Smartphone einer Benutzerin oder eines Benutzers mit Schadsoftware infiziert hat, die ihm den Zugriff auf das Mikrofon oder gespeicherte Daten des Mikrofons erlaubt. Prinzipiell können dabei die gleichen akustischen Informationen wie in B4.3.a kompromittiert werden. Da eine persönliche Anwesenheit des Angreifers in diesem Szenario nicht nötig ist, geht hiervon eine größere Bedrohung aus als bei B4.3.a.

A4.4	**Interne Kommunikationsschnittstellen**: Interne Kommunikationsschnittstellen der zentralen Infrastruktur können Zugriff auf interne Services und damit auch auf kritische Daten erlauben. Beispiele für derartige Schnittstellen sind Netzwerkbuchsen aber auch WLAN-Access-Points.
B4.4	**Zugriff auf interne Kommunikationsschnittstellen**: Angreifer können Smartphones benutzen, um interne Kommunikationsschnittstellen wie WLANs zu scannen und relevante netzwerkbezogene Informationen zu sammeln. Dieses Bedrohungsszenario ist prinzipiell nicht auf eine Verwendung von Smartphones beschränkt, deren Mobilität und Unauffälligkeit kann derartige Angriffe für Angreifer jedoch signifikant erleichtern.

A4.5	**Smartphone Management**: Über die Smartphone-Management-Komponente können allgemein gültige Policies für Smartphones festgelegt werden. Da diese Policies die sichere Verwendung von Smartphones im Rahmen einer Smartphone-Infrastruktur gewährleisten, ist diese Komponente als relevantes Asset zu betrachten. Diese Komponenten sind ausschließlich in Unternehmensinfrastrukturen, in denen Smartphones vom Unternehmen an Mitarbeiter ausgegeben werden, verfügbar. Im Rahmen von Smartphone-basierten E-Government Diensten hat die Behörde in der Regel keine Handhabe über die von Benutzerinnen und Benutzern der Dienste verwendeten Endgeräte.
B4.5	**Zugriff auf das Smartphone Management**: Erhält ein Angreifer Zugriff auf die Smartphone-Management-Komponente, kann er unter Umständen Policies einsehen oder verändern und so Sicherheitsvorkehrungen außer Kraft setzen.

A.4.3 Schutzfunktionen

Die Sicherheit der verschiedenen für Smartphone-Infrastrukturen definierten Assets wird durch eine Vielzahl an Bedrohungen gefährdet. Zur Abwendung dieser Bedrohungen stehen verschiedenste Sicherheits- bzw. Schutzfunktionen zur Verfügung. Schutzfunktionen finden sich dabei in allen drei Hauptbereichen von Smartphone-Infrastrukturen: Zentrale Infrastruktur, Kommunikation und Smartphone-Plattform. Das Ziel sämtlicher Schutzfunktionen ist im Allgemeinen stets die Sicherung des Primär-Assets „Daten“. Diese sollten durch geeignete Maßnahmen vor unerlaubtem Zugriff und Modifikation geschützt werden. Erreicht wird dies je nach Art der Bedrohung durch unterschiedliche Funktionen und Mechanismen, die jedoch stets nur auf ein Subset aller Bedrohungen anwendbar sind.

In diesem Abschnitt werden die einzelnen verfügbaren Schutzfunktionen näher beschrieben. Hauptaugenmerk wird dabei auf Smartphone-Plattformen und die für mobile Endgeräte verfügbaren Sicherheitsfunktionen gelegt. Damit zeigt dieser Abschnitt Strategien auf, die Unternehmen aber auch Privatpersonen in der Abwehr Smartphone-bezogener Bedrohungen unterstützen können.

A.4.3.1 Smartphone Plattform

Aufgrund ihrer Exponiertheit stellen mobile Endgeräte in der Regel den verwundbarsten Bereich einer Smartphone-Infrastruktur dar. Aufgrund der vielen technologischen Möglichkeiten und Funktionen von Smartphones ergeben sich für Angreifer neue Varianten, diese Funktionalität für bösartige Aktivitäten auszunutzen. Gleichzeitig bieten Smartphones jedoch auch zahlreiche Funktionen zum Schutz gegen derartige Bedrohungen.

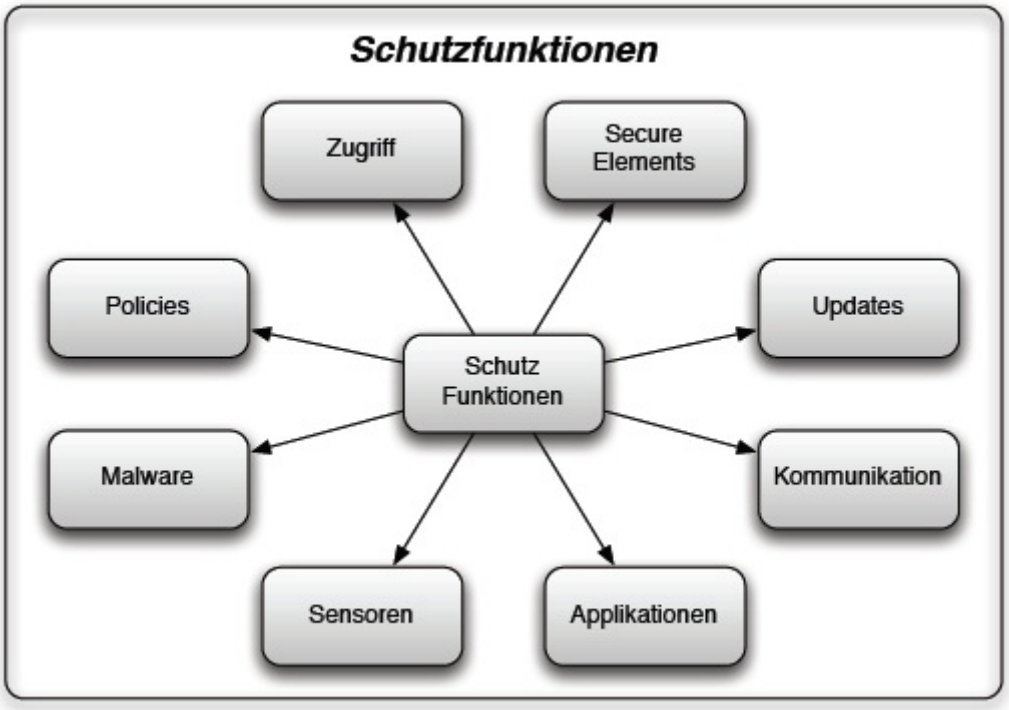

Abbildung A.4.8: Smartphone Schutzfunkionen

A.4.3.1.1 Applikationsschutz

Die Möglichkeit eine Vielzahl an Applikationen (Apps) am mobilen Gerät betreiben zu können ist einer der größten Vorteile von Smartphones. Gleichzeitig bringt diese Flexibilität jedoch auch zahlreiche Gefahren mit sich. Je nach Art der Applikation kann diesen Gefahren mit verschiedenen Schutzfunktionen begegnet werden. Relevante diesbezügliche Schutzfunktionen sind in Abbildung A.4.9 skizziert und über die untenstehende Aufzählungsliste überblicksmäßig beschrieben.

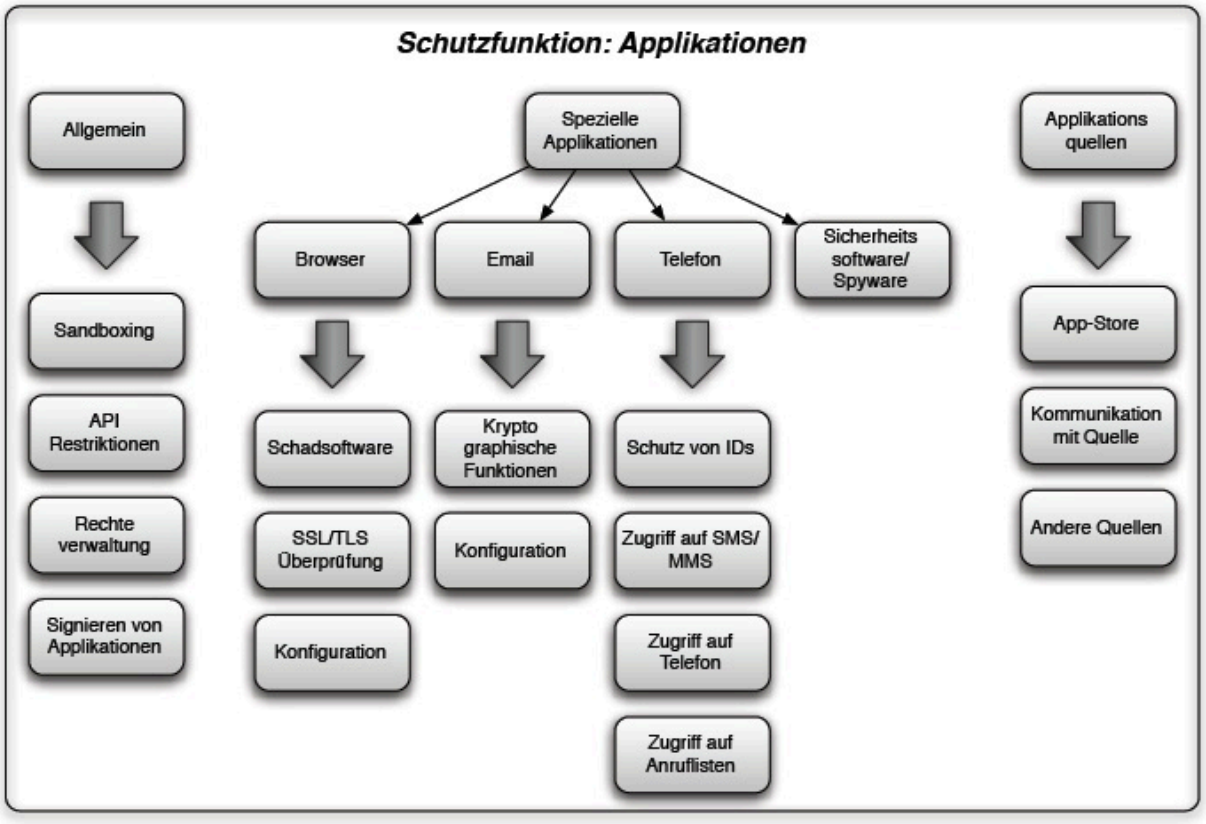

Abbildung A.4.9: Schutzfunktionen Applikationen

- **Allgemeine Schutzfunktionen:** Moderne Smartphone-Plattformen unterstützen von Haus aus eine Reihe von Schutzfunktionen, über die die Sicherheit von Applikationen (Apps) auf Smartphones erhöht wird. Dazu zählen vor allem:
  - **Sandboxing:** Smartphone-Apps sind voneinander weitgehend isoliert und können nur sehr eingeschränkt miteinander kommunizieren. Ein positiver Effekt daraus ist, dass die Kompromittierung einer App nicht notwendigerweise zu einer Kompromittierung anderer Apps am selben Gerät führt. Auch haben böswillige Apps nur wenig Möglichkeiten, Schaden in anderen Apps anzurichten.
  - **API-Restriktionen:** Apps haben nur eingeschränkte Möglichkeiten APIs der Smartphone-Plattform zu verwenden. Dies minimiert wiederum das Schadenspotenzial böswilliger Apps.
  - **Rechteverwaltung:** Apps haben standardmäßig nur sehr wenige Berechtigungen. Benutzerinnen und Benutzer müssen der Zuweisung zusätzlicher Berechtigungen explizit zustimmen und behalten so die Kontrolle über die Befugnisse installierter Apps.
  - **Signieren von Applikationen:** Apps müssen vom Hersteller signiert sein. Damit ist die Authentizität von Apps gewährleistet und die Verwendung unautorisiert modifizierter Apps wird unterbunden.

    - **Geräteverschlüsselung:** Die geräteweite Datenverschlüsselung erhöht indirekt auch die Applikationssicherheit, da Applikationsdaten so vor Kompromittierung geschützt werden.
- **Absicherung des Web-Browsers:** Auch auf mobilen Endnutzergeräten wie Smartphones spielt der Web-Browser eine wichtige Rolle. Dementsprechend ist auch seine Sicherheit von zentraler Bedeutung. Die Sicherheit des Web-Browser kann unter anderem über folgende Methoden erhöht werden:
    - **Schutz vor Schadsoftware:** Aufgrund seiner zentralen Rolle ist der Web-Browser ein attraktives Ziel von Schadsoftware. Ein Schutz gegen solche Schadsoftware ist damit ein wichtiger Baustein für die Sicherheit des Web-Browsers.
    - **Überprüfung von TLS/SSL Zertifikaten:** Es sollte gewährleistet werden, dass verwendete Web-Browser im Rahmen des Aufbaus von TLS-Verbindung (bzw. DTLS-Verbindungen) die zum Einsatz kommenden Zertifikate und ihre Gültigkeit verlässlich prüfen.
    - **Konfiguration:** Es muss auf eine adäquate Konfiguration des Web-Browsers geachtet werden. Vor allem sicherheitsbezogene Konfigurationen müssen so gesetzt werden, dass eine sichere Verwendung des Web-Browser und eine sichere Konsumierung von Web-Content gewährleistet ist.
- **Absicherung des E-Mail-Verkehrs:** Trotz der stetigen Verbreitung von Messenger-Lösungen spielt E-Mail als Kommunikationstechnologie vor allem im Unternehmensumfeld auch auf Smartphones nach wie vor eine gewichtige Rolle. In Anbetracht der Tatsache, dass über E-Mail oft auch kritische Daten übertragen werden, ist die Absicherung dieses Kommunikationskanals von besonderer Bedeutung. Hierfür bieten sich im Allgemeinen vor allem folgende Schutzfunktionen an:
    - **Kryptographische Funktionen:** Die Vertraulichkeit und Integrität von E-Mails kann durch die Verwendung kryptographischer Methoden (S/MIME, PGP etc.) sichergestellt werden. Zu beachten ist ein oft zu beobachtender Trade-off zwischen Sicherheit und Benutzerfreundlichkeit.
    - **Konfiguration:** Ein Mindestmaß an Sicherheit kann schon durch eine geeignete Konfiguration des E-Mail-Systems erreicht werden (z.B. betreffend der geschützten Übertragung von Anmeldedaten, etc.).
- **Absicherung der Telefonapplikation:** Auch wenn auf modernen Smartphones Telefonie nur mehr eine von vielen Funktionen ist, sollte diese ausreichend abgesichert werden. Dies betrifft vor allem Aspekte des Zugriffschutzes, wie z.B.:
    - Schutz vor Zugriff auf die IDs
    - Schutz vor Zugriff auf SMS-Nachrichten
    - Schutz vor Zugriff auf Telefonfunktionalität
    - Schutz vor Zugriff auf Anruflisten

- **Schutz von Applikationsquellen:** Ein Unterscheidungsmerkmal von Smartphones im Vergleich zu klassischen Endnutzergeräten ist die Verwendung von App-Stores, über die Anwendungen zentral bezogen werden können bzw. müssen. Neben den offiziellen App-Stores der Smartphone-Plattformen können optional auch noch weitere Applikationsquellen zum Einsatz kommen. In jedem Fall müssen diese Quellen ausreichend abgesichert sein, sodass sichergestellt ist, dass nur legitime Apps auf Endgeräten zur Installation und Anwendung kommen. Dies betrifft im Wesentlichen folgende Aspekte:
    - **Schutzfunktionen des App-Stores:** App-Stores implementieren in der Regel eine Reihe von Schutzfunktionen zur Vermeidung der Verbreitung von böswilligen Apps. Unter anderem müssen Apps, die über offizielle App-Stores bereitgestellt werden, einen Review-Prozess durchlaufen.
    - **Absicherung der Kommunikation mit dem App-Store:** Es muss sichergestellt sein, dass die Sicherheit von Apps im Zuge ihrer Übertragung vom App-Store zum mobilen Gerät gewährleistet ist.
    - **Andere Quellen:** Die Verwendung alternativer Quellen für Apps sollte wohlüberlegt und nur bei Vorliegen guter Gründe in Betracht gezogen werden. Werden alternative Quellen selbst bereitgestellt, muss deren Sicherheit gewährleistet werden. In keinem Fall sollten Apps von nicht vertrauenswürdigen alternativen Quellen bezogen werden.
- **Sicherheitssoftware und Spyware:** Der Einsatz von Sicherheitssoftware kann sich als zweischneidiges Schwert erweisen. Legitime Sicherheitssoftware kann die Sicherheit am Smartphone prinzipiell schon erhöhen, allerdings muss diese in der Regel mit weitgehenden Berechtigungen ausgestattet werden, wodurch diese auch die technischen Voraussetzungen für eine Spyware mitbringt. Sicherheitssoftware sollte daher noch mehr als andere Apps nur von tatsächlich vertrauenswürdigen Anbietern bezogen werden.

A.4.3.1.2 Schutz der Sensordaten

Smartphones sind in der Regel mit einer Vielzahl unterschiedlicher Sensoren ausgestattet. Die von diesen Sensoren gesammelten und aufgezeichneten Daten können vertraulicher Natur sein. Ein adäquater Schutz dieser Daten ist daher für die Gesamtsicherheit von Smartphone-Plattformen unumgänglich. Im Speziellen sind folgende Aspekte zu betrachten:

- **Zugriffschutz auf Sensoren:** Der Zugriff auf Sensoren wird über Berechtigungen gesteuert. Diese sollten dementsprechend wohlüberlegt vergeben werden.
- **Schutz von Sensordaten:** Sensordaten werden vom mobilen Betriebssystem und installierten Apps verarbeitet und gespeichert. Da es sich hier um potenziell kritische Daten handelt, sollten diese im Zuge der Verarbeitung und Speicherung ausreichend geschützt werden. Siehe dazu auch relevante Aspekte des Abschnitts zu Applikationsschutz.

- **Anzeige aktiver Sensoren:** Moderne Smartphones zeigen in der Regel an, welche Sensoren gerade aktiv sind. Hier ist dementsprechend ein entsprechendes Bewusstsein bei Benutzerinnen und Benutzern gefragt, um den Einsatz von Sensoren laufend zu überwachen.

A.4.3.1.3 Schutz vor Schadsoftware

Smartphones sind aufgrund ihres mittlerweile beträchtlichen Funktionsumfangs klassischen Endnutzergeräten wie Desktop-PCs und Laptops sehr ähnlich. Damit sind für Smartphones auch diverse Probleme ein Thema, die für herkömmliche Mobiltelefone noch gänzlich irrelevant waren. Dies betrifft vor allem den Umgang mit Schadsoftware wie Viren, Würmer und Trojaner, für welche auf Smartphones einige Schutzfunktionen existieren. Diese sind in Abbildung A.4.10 dargestellt und im Folgenden gelistet.

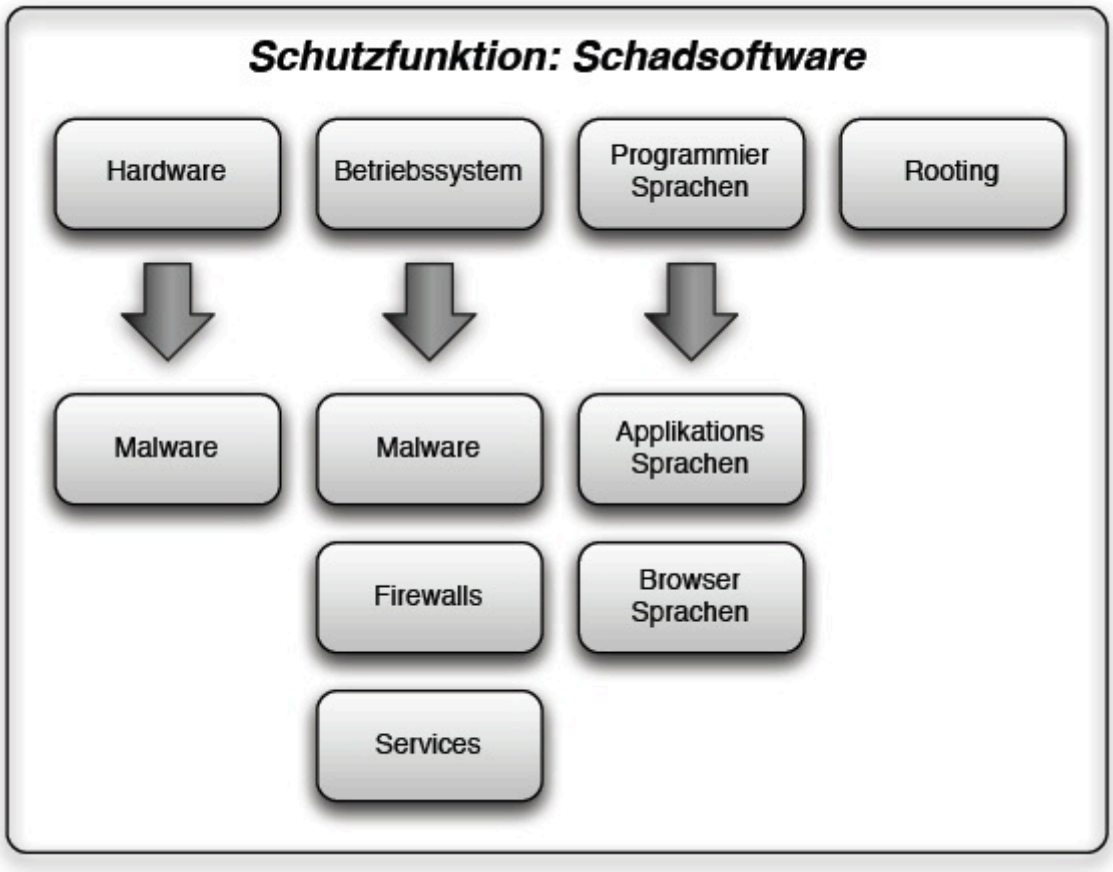

Abbildung A.4.10: Schutzfunktionen Schadsoftware

- **Schutzmechanismus der Hardware:** Bereits auf Hardwareebene existieren Schutzfunktionen gegen Malware. Zu nennen ist hier beispielsweise der hardwareunterstützte Verified-Boot-Process, über den beginnend beim Bootloader die Signaturen sämtlicher gestarteter Softwarekomponenten gegen den Root-of-Trust des Herstellers validiert wird.
- **Schutzmechanismus des Betriebssystems:** Auch auf Betriebssystemebene existieren Schutzmechanismen vor Malware, wie zum Beispiel Firewalls oder dezidierte Services.
- **Programmiersprachen:** Schutz vor Malware kann auch durch die geeignete Wahl von Programmiersprachen erreicht werden. Relevant sind hier vor allem:
    - **Sprachen für Applikationen:** Es sollten jene Sprachen bei der Entwicklung von Apps gewählt werden, die die Wahrscheinlichkeit von Fehlern (Bugs), die von Malware ausgenutzt werden könnten, minimieren.
    - **Sprachen im Browser:** Auch bei der Entwicklung von Browser-Applikationen sollten geeignete Sprachen gewählt werden, die Möglichkeiten von Malware weitestgehend einschränken.
    - **Schutz vor Rooting:** Applikationen sollten im Idealfall sogenannte Root-Checks integrieren, über die überprüft wird, ob das Smartphone gerootet wurde und damit von der korrekten Funktion diverser integrierter Sicherheitsmechanismen nicht mehr ausgegangen werden kann.

A.4.3.1.4 Zugriffsschutz

Ein Vorteil und Risiko zugleich ist die Mobilität von Smartphones. Da diese von einer Benutzerin oder einem Benutzer meist mitgeführt werden, ist das Risiko für Verlust oder Diebstahl ungleich größer als bei stationären Geräten wie Desktop PCs. Mit dem Verlust des Smartphones fallen einem Finder oder Dieb potenziell auch sämtliche am Smartphone gespeicherten Daten in die Hände. Ein geeigneter Schutz der am Smartphone gespeicherten Daten ist daher unbedingt notwendig. Folgende Aspekte können zu diesem Schutz beitragen:

- **Datenverschlüsselung:** Moderne Smartphones unterstützen eine systemweite Verschlüsselung von Daten.
- **Sperre des Smartphone:** Smartphones unterstützen diverse Methoden des Zugriffsschutzes. Dazu zählen PINs, Passwörter oder auch biometrische Verfahren.
- **Remote Wipe/Location:** Für den Fall des Verlusts oder Diebstahls des Smartphones unterstützen moderne Smartphones Methoden der Lokalisierung oder auch der entfernten Datenlöschung.
- **Schutz von Zugangsdaten:** Smartphones unterstützen hardwaregestützte Methoden zur sicheren Speicherung von Zugangsdaten am mobilen Gerät.

A.4.3.1.5 Policies

Eine sehr wichtige Komponente für die Sicherheit einer Smartphone-Plattform, die in einem Unternehmen oder im Rahmen von E-Government Anwendungen in einer Behörde eingesetzt wird, ist ein Policy-Management-Framework. Diese Technologie ermöglicht das Vorschreiben technischer Sicherheitsmaßnahmen und deren zwingende Umsetzung auf verwendeten Smartphones. Benutzerinnen und Benutzer haben in der Regel keine Möglichkeit diese Vorgaben zu ändern. Dies spielt vor allem im Bereich Verschlüsselung, bei der Vorgabe von Mindestlängen bei PINs und Passwörtern, oder beim Installieren von externen Applikationen eine Rolle. Abhängig vom Hersteller existieren auch noch tiefergehende Policies, die alle Funktionen eines Smartphones abdecken können. Ein Policy-Framework ist beim Einsatz einer Smartphone-Plattform in Unternehmen und Behörden unabdingbar, da nur so eine existierende IT-Security-Policy auf Smartphones abgebildet werden kann.

A.4.3.1.6 Secure Elements

Secure Elements bergen aus sicherheitstechnischer Sicht ein großes Potenzial. Diese Hardwarekomponenten können einerseits als sicherer Schlüsselspeicher fungieren und stellen andererseits eine Reihe kryptographischer Operationen zur Verfügung. Mit Hilfe von Secure Elements können daher verschiedene auf Kryptographie basierende Schutzmechanismen implementiert werden. Diese werden genutzt, um die Integrität des Betriebssystems und die der darauf installierten Apps zu gewährleisten. Dadurch wird die Sicherheit der gesamten Smartphone-Plattformen erhöht.

A.4.3.1.7 Updates

Ein funktionierender Update-Mechanismus stellt ebenfalls eine wichtige Schutzfunktion dar. Da die Erstellung fehlerfreier Software in der Realität kaum zu erfüllen ist, ist die Möglichkeit einer schnellstmöglichen Korrektur entdeckter Fehler und Sicherheitslücken umso wichtiger. Zuverlässige Updatemechanismen gewährleisten, dass aktualisierte und verbesserte Version von Softwarekomponenten rasch und zuverlässig an die einzelnen mobilen Endgeräte übermittelt und auf diesen installiert werden können. Dadurch können Smartphones stets auf einem aktuellen Stand gehalten und deren Sicherheit gewährleistet werden.

A.4.3.2 Kommunikation

Der Kommunikationspfad zwischen zentraler Infrastruktur und Smartphone stellt den zweiten Hauptbereich einer Smartphone-Infrastruktur dar. Über diesen Kommunikationspfad werden Daten zwischen zentralen Komponenten und entfernten mobilen Geräten ausgetauscht. Die Datenübertragung erfolgt dabei in der

Regel über drahtlose Kommunikationsprotokolle. Um ein Abhören der übertragenen Daten zu unterbinden, ist die Anwendung verschiedener Schutzmaßnahmen nötig. Auf die verschiedenen verfügbaren Maßnahmen zur Absicherung der Kommunikation zwischen zentraler Infrastruktur und mobilen Endgeräten wird in diesem Abschnitt näher eingegangen.

A.4.3.2.1 Schutz von Kommunikationskanälen

Die verschiedenen von Smartphones verwendeten mobilen Kommunikationskanäle bieten unterschiedliche Möglichkeiten der Absicherung. Im Folgenden werden Schutzfunktionen der am häufigsten verwendeten Kommunikationstechnologien diskutiert.

- **WLAN:** Zur Absicherung der Kommunikation über WLAN stehen diverse erprobte Protokolle zur Verfügung. Als Beispiel kann hier der Wi-Fi Protected Access (WPA) Standard bzw. dessen Nachfolger WPA2 und WPA3 genannt werden. Basierend auf kryptographischen Methoden ermöglichen diese Protokolle eine sichere Kommunikation über drahtlose Netzwerke. Auf Seiten der Smartphone-Plattform ist dazu die Unterstützung dieser Protokolle und Standards notwendig.
- **Bluetooth:** Bluetooth stellt eine Kommunikationsmethode dar, mit der das Smartphone über kurze Entfernungen mit anderen Geräten kommunizieren kann. Anwendungsbeispiele sind Freisprecheinrichtungen, der Austausch von Kontaktdaten, der Transfer von Daten oder das Anbieten einer Internetanbindung für ein anderes Gerät (Tethering). Zur Absicherung von Bluetooth-Verbindungen ist vor allem auf eine geeignete Wahl der Bluetooth-Einstellungen und die Sicherheit des Pairing-Prozesses zu achten.
- **Mobilfunk:** Die gängigen Mobilfunkprotokolle GSM, UMTS (3G), LTE (bzw. 4G) und 5G sind die Basistechnologien, die für den Zugang zum Internet verwendet werden. Vor allem für GSM sind viele Sicherheitsprobleme bekannt. Um einen adäquaten Schutz übermittelter Daten zu erreichen, ist die Verwendung kryptographischer Methoden auf höheren Abstraktionsebenen nötig.
- **NFC:** NFC kommt vor allem in Spezialanwendungen wie dem bargeldlosen Bezahlen oder zur Herstellung von Verbindungen zwischen mobilen Geräten zur Anwendung. Durch die Verwandtschaft von NFC zur RFID-Technologie können einige der für RFID entwickelten Sicherheitsmechanismen auch für NFC-basierte Kommunikation verwendet werden.

A.4.3.2.2 VPN

Virtuelle private Netzwerke (VPN) bieten die Möglichkeit, durch Verwendung kryptographischer Verfahren abgesicherte Netzwerke auf ursprünglich unsicheren Netzen zu betreiben. Damit können beispielsweise Endgeräte wie PCs, Laptops, aber auch Smartphones über eine abgesicherte Verbindung an zentrale Netze

angebunden werden. Virtuelle private Netzwerke können über unterschiedliche Protokolle implementiert werden. Zu den häufigsten verwendeten Protokollen zählen dabei IPsec, L2TP und PPTP. VPN stellt eine wichtige Schutzfunktion dar, um einen sicheren Datenaustausch über potenziell unsichere Netzwerke zu ermöglichen.

A.4.3.2.3 Benachrichtigungen (Push-Services)

Push-Services werden von Plattformherstellern benutzt, um Benachrichtigungen an Smartphones zu schicken. Dabei können die hier eingesetzten Technologien und Anwendungen unterschiedlichster Natur sein. Vor allem für Applikationsentwickler ist aber wichtig, wie ein Push-Service abgesichert ist, wenn kritische Informationen an Applikationen übermittelt werden sollen.

A.4.3.3 Zentrale Infrastruktur

Zentrale Infrastrukturen werden meist in entsprechend abgesicherten Rechenzentren betrieben. Der Schutz von Rechenzentren bedarf umfassender Maßnahmen, auf die im Rahmen dieses Anhangs nicht im Detail eingegangen werden soll. In der Regel wird die Gewährleistung eines adäquaten Sicherheitsniveaus beim Betrieb von Rechenzentren ohnehin durch externe Audits anhand bewährter nationaler und internationaler Standards überprüft. Durch die Integration von Smartphones in bestehende Infrastrukturen können sich jedoch zusätzliche Risiken ergeben. Im Folgenden sollen diverse Schutzfunktionen, mit denen diesen Risiken auf zentraler Seite begegnet werden kann, diskutiert werden.

A.4.3.3.1 Smartphone-Plattform

Bevor eine Smartphone-Plattform in Unternehmen oder Behörden eingesetzt werden kann, müssen die Sicherheitsfeatures der geplanten Verwendung gegenübergestellt werden. Dabei müssen alle bisher diskutierten Schutzfunktionen überprüft werden.

A.4.3.3.2 IT-Sicherheits-Policy und Schulungen

Da sich Smartphones durch ihre Mobilität sowohl in Bezug auf Möglichkeiten als auch in Bezug auf Gefahren signifikant von anderen mobilen Geräten wie Laptops unterscheiden, muss eine an Smartphones angepasste Sicherheits-Policy erstellt werden. Die für Mitarbeiterinnen und Mitarbeiter relevanten Punkte und potenzielle Gefahren bei Smartphones müssen in geeigneter Weise (z.B. in Form von Schulungen) vermittelt werden, um so ein Bewusstsein für die Gefahren im Umgang mit Smartphones zu schaffen. Nur wenn sich sämtliche Mitarbeiterinnen und Mitarbeiter eines Unternehmens oder einer Behörde über Bedrohungen und entsprechende Gegenmaßnahmen im Klaren sind, kann die Sicherheit von Smartphone-Infrastrukturen gewährleistet werden.

A.4.3.3.3 VPN-Unterstützung

Wie auch weiter oben erläutert, spielt die VPN Technologie eine entscheidende Rolle bei der sicheren Anbindung von Smartphones an zentrale Infrastrukturen. Eine Unterstützung dieser Technologie und die Bereitstellung und Wartung entsprechender VPN-Entry-Points stellt daher auch für zentrale Infrastrukturen eine wichtige Schutzfunktion dar. Für den Fall, dass die verwendeten VPNs korrekt konfiguriert sind und die für den externen Zugang verwendeten Zugangsdaten ausreichend geschützt bleiben, bietet VPN eine sichere und zuverlässige Möglichkeit der Anbindung externer Komponenten. Ein kompromittierter VPN-Zugang stellt hingegen eine ernstzunehmende Bedrohung für die Sicherheit der gesamten Smartphone-Infrastruktur dar. Eine ausreichende Absicherung der gesamten VPN-Infrastruktur ist daher eine zwingende Voraussetzung für den erfolgreichen Einsatz von VPN als Schutzfunktion.

A.4.3.3.4 Zonen

Eine Verbindung von Smartphones zum Unternehmen oder zur Behörde wird dann benötigt, wenn diese auf Daten oder Dienste des Unternehmens oder der Behörde zugreifen müssen. Dabei handelt es sich entweder um den Zugriff auf die E-Mail-Server des Unternehmens oder um den Zugriff auf interne Dienste via Browser oder eigenen am Smartphone installierten Applikationen. Dabei muss das Smartphone also einen Zugriff auf das interne Netzwerk haben. Durch eine wohlüberlegte Segmentierung des Netzwerks in unterschiedliche Zonen können Risiken, die sich aus einem Smartphone-Zugriff ergeben können, minimiert werden. Beispielsweise kann so ein Zugriff auf bestimmte Zonen mit geringerer Kritikalität eingeschränkt werden.

A.4.3.3.5 Verwaltung

Um Smartphones verwalten zu können, muss typischerweise ein dedizierter Server in der zentralen Infrastruktur eingesetzt werden. Da die dafür benötigten Daten wie Policies oder Schlüsselmaterial unbedingt geschützt werden müssen, ist sicherzustellen, dass der Server so in das Unternehmensnetzwerk integriert ist, dass Angriffe verhindert werden können.

A.4.3.3.6 E-Mail-Anbindung

Smartphones werden typischerweise auch für den mobilen Zugriff auf E-Mail-Server des Unternehmens oder der Behörde verwendet. Dabei muss davon ausgegangen werden, dass E-Mails vertrauliche Daten enthalten, die eine sichere Verwendung unbedingt nötig machen.

A.5 Sicherheit in sozialen Netzen

Beim vorliegenden Anhang handelt es sich um das Ergebnis eines Semesterprojekts von Studenten der Fachhochschule Hagenberg. Dieser Anhang beschäftigt sich mit dem korrekten Umgang von Unternehmen und deren Mitarbeiterinnen und Mitarbeitern bezüglich sozialer Netze. Es stützt sich auf Vorgaben aus dem Österreichischen Informationssicherheitshandbuch, sowie weiteren Quellen die im folgenden angeführt sind:

- *Bundesamt für Sicherheit in der Informationstechnik: Basismaßnahmen der Cyber-Sicherheit*
- *Bundesamt für Sicherheit in der Informationstechnik: BSI für Bürger: Sichere Soziale Netze*
- *E-Government Bund-Länder-Gemeinden: E-Democracy: Entscheidungsgrundlage für die Nutzung von Soziale Medien & Netzwerken in der Verwaltung, Soziale Medien & Netzwerke in der Verwaltung*
- *E-Government Bund-Länder-Gemeinden: E-Democracy: Leitfaden – Umgang mit Web 2.0 für MitarbeiterInnen der öffentlichen Verwaltung, BeamteZweiNull*
- *Heidrich, Joerg; Kuri, Jürgen: Social Media Guidelines. In: c't extra: soziale Netze. (Oktober 2012), S. 176-179*
- *ISACA: Social Media: Business Benefits and Security, Governance and Assurance Perspectives*
- *Schweizerische Kriminal Prävention - Prévention Suisse de la Criminalité: Checkliste: Sicherheit in Sozialen Netzwerken*
- *Stadt Wien: Social Media Richtlinien für die Stadt Wien: Stadt Wien Social Media Manual – Leitfaden für die verantwortungsvolle Kommunikation im Web 2.0 und in Sozialen Medien*
- *Stadt Wien: Social Media Richtlinien für die Stadt Wien: Stadt Wien Social Media Manual – Leitfaden für die Öffentlichkeitsarbeit von Dienststellen im Web 2.0 und in Sozialen Medien*
- *Tantau, Björn: Facebook Monitoring bei Daimler unbekannt*
- *Tantau, Björn: Fünf Gründe gegen Social Crossposting*s
- *Verein für Konsumenteninformation (VKI): Soziale Netzwerke, Foren & Co. In: Ihr Recht im Internet (2011), S. 95-105*

A.5.1 Einführung

Soziale Netze gewinnen zunehmend an Bedeutung. Längst sind nicht mehr nur Privatanwender die Nutzer sozialer Netze, sondern Unternehmen und Behörden haben die Vorteile, die sich aus der Nutzung sozialer Netze ergeben, für sich entdeckt, insbesondere für die Bereiche Marketing und Öffentlichkeitsarbeit.

Daraus ergeben sich Anforderungen an die IT-Sicherheit, damit ein sicherer und seriöser Auftritt einer Organisation sowie der Schutz der beruflichen Profile der Nutzer auf den Plattformen gewährleistet ist. MitarbeiterInnen müssen für den Umgang mit sozialen Netzen sensibilisiert werden. Dies beinhaltet verbindliche Vorgaben für das Verhalten in sozialen Netzen (Social Media Guidelines). Besonders in Bezug auf Behörden müssen die vorhandenen Nutzungsbedingungen sowie Erlässe zur Nutzung der IT-Infrastruktur auf Länder- und Bundesebene beachtet werden.

Sicherheitsmaßnahmen, die seitens sozialer Netze angeboten werden, müssen allen MitarbeiterInnen, die beruflich mit sozialen Netzen umgehen, bekannt sein, und entsprechend angewandt werden. Ebenso müssen Grenzen der IT-Sicherheit in sozialen Netzen bekannt sein, wie etwa, dass Informationen, die einmal in das soziale Netz gegeben wurden, aus diesem nicht mehr gänzlich zu löschen sind.

A.5.1.1 Rechtlicher Hintergrund

In der Vergangenheit kam es bereits zu Rechtsstreitigkeiten im Zusammenhang mit sozialen Netzen und MitarbeiterInnen. Dabei standen vor allem negative Äußerungen über das Arbeitsverhältnis und preisgegebene, firmeninterne Informationen im Vordergrund. In einigen Fällen entschied das zuständige Gericht zugunsten des Arbeitgebers, was oftmals eine Kündigung und teilweise weitere arbeitsrechtliche Konsequenzen zur Folge hatte. Um solche Vorfälle zu vermeiden müssen verbindliche Social Media Guidelines existieren.

Ein weiterer Streitpunkt kann die Besitzzugehörigkeit eines Nutzerkontos, das für den Auftritt der Organisation im sozialen Netz verwendet wird, sein. Dies gilt insbesondere bei Beendigung des Dienstverhältnisses des Mitarbeiters, der das betreffende Nutzerkonto für die Organisation verwendet hat. Es ist zu klären, wem die Community, die Kontakte und Zugangsdaten gehören, die mit dem Nutzerkonto verknüpft sind. Besonders schwierig ist dies, wenn für die berufliche Kommunikation ein privates Nutzerkonto verwendet wurde. Insbesondere wenn dieses Nutzerkonto privat finanziert wurde, beispielsweise durch eine Premiumoption im sozialen Netz. Schon aus diesem Grund ist ein eigens für die berufliche Verwendung angelegtes Nutzerkonto unverzichtbar.

Ein zusätzlicher Aspekt, der beachtet werden muss, ist die derzeit gültige Rechtslage – zum Beispiel die Verpflichtung zur Offenlegung eines Impressums (vgl. § 25 Mediengesetz), oder die gesetzliche Verpflichtung des barrierefreien Zugangs zu einem Internetauftritt einer Behörde (vgl. § 1 Abs. 3 E-Government-Gesetz), welcher bei externen Diensten oftmals nicht gewährleistet werden kann.

A.5.1.2 Datenschutz

Bei Verwendung von sozialen Netzen im Arbeitsumfeld muss sich die Organisation bewusst sein, dass sämtliche Daten, die seitens des Unternehmens in das soziale Netz fließen, auf unbestimmte Zeit und außerhalb der Kontrolle der Organisation gespeichert werden. Zwar können Daten aus dem öffentlichen Raum entfernt werden, sie bleiben jedoch häufig auf den Servern des sozialen Netzes gespeichert.

Das gültige Recht für die gespeicherten Daten ist nicht gänzlich geklärt. Der Verein für Konsumenteninformation (VKI) stellt dazu etwa fest: „Wenn Daten in Österreich verwendet werden, muss dies grundsätzlich nach den Regeln des österreichischen Datenschutzgesetzes (DSG) geschehen. In vielen Fällen sitzt der Betreiber einer Plattform jedoch nicht in Österreich, eventuell hat er nicht einmal eine Niederlassung innerhalb der Europäischen Gemeinschaft. In diesen Fällen ist fraglich, ob überhaupt das österreichische Datenschutzgesetz gilt. Die Gerichte haben das bislang nicht geklärt. Dennoch ist es sicherlich kein Fehler, sich bei Auseinandersetzungen (auch) auf die Geltung des österreichischen Datenschutzgesetzes zu berufen, da die Dateneingabe ja auf Ihrem Computer erfolgt, der sich in Österreich befindet“.

Oftmals verwenden soziale Netze bewusst Länder, in denen die Gesetze zum Datenschutz für ihre Zwecke günstig sind. Diese weisen dann gravierende Unterschiede zum Datenschutzgesetz in Österreich auf, und sollten im Einzelfall geprüft werden.

A.5.1.3 Datensicherheit

Neben den rechtlichen Aspekten des Datenschutzes ist auch die Sicherheit der Daten entscheidend. Das soziale Netz hat die Daten auf seinen Servern gespeichert, wodurch die Sicherheit dieser Informationen im großen Maß von der Sicherheit des sozialen Netzes abhängt. Die Organisation, die die Daten in das soziale Netz gespeist hat, verliert mit dem Abschicken jegliche Kontrolle oder Einfluss über die Daten. So könnten bei einem Angriff auf das soziale Netz Daten, die zuvor nur einem kleinen Kreis an Nutzern im sozialen Netz sowie dem Betreiber zugänglich waren, in die Hände Dritter fallen.

A.5.1.4 Protokollierung von Kommunikation in sozialen Netzen

Die Überwachung des Fernmeldeverkehrs durch den Arbeitgeber ist in Österreich eine rechtliche Grauzone, für die es derzeit keine klare Lösung gibt. Es hat sich etabliert eine geringfügige private Nutzung zu tolerieren, sofern die Organisation keine sehr hohen Ansprüche an Sicherheit und Geheimhaltung erfordert.

Siehe Kapitel 12.5.4 Rechtliche Aspekte bei der Erstellung und Auswertung von Protokolldateien zur E-Mail- und Internetnutzung.

A.5.1.5 Monitoring

Als Monitoring, Screening oder Tracking von sozialen Netzen werden neben dem Überwachen von Diskussionen auf beleidigende, rassistische, pornografische oder verbotene Inhalte auch die Mitverfolgung und statistische Auswertung von Inhalten, die die Organisation betreffen, bezeichnet. Dies kann zum einen zur Erfassung und Kontrolle der Reputation der Organisation im Netz genutzt werden, zum anderen aber auch, um die Aktivitäten der eigenen Mitarbeiter mit ihrem Firmen- bzw. Behördenbenutzerkonto innerhalb der sozialen Netze nachzuverfolgen und entsprechend zu reagieren.

Szenario zu den möglichen Auswirkungen, wenn auf Monitoring verzichtet wird

Eine Organisation betreibt seit einiger Zeit erfolgreich Auftritte in sozialen Netzen. Aufgrund der positiven Aufnahme durch Kunden sowie belegbarer Erfolge nimmt die Zahl der Mitarbeiter stark zu, die in diesen sozialen Netzen offizielle Benutzerkonten der Organisation erhalten.

Eine kürzlich getätigte politische Entscheidung der Regierung, die die Bevölkerung in ihrer Meinung in unterschiedliche Lager teilt, veranlasst viele Menschen zu Protestbewegungen, auch im Netz. Einige Mitarbeiter der Organisation unterstützen nun in den sozialen Netzen diese Protestbewegung mit ihrem Firmen- bzw. Behördenbenutzerkonto, obwohl dies gegen die Richtlinien der Organisation verstößt. Nach und nach schließen sich immer mehr Mitarbeiter an.

Erst als mehrere Kunden, verwundert über die politische Aktivität, bei der Organisation nachfragen, gelangt die Information an den zuständigen Abteilungsleiter, der daraufhin die betroffenen MitarbeiterInnen zu einem Gespräch bittet.

Wenn die Organisation Monitoring eingesetzt hätte, um die Aktivitäten seiner MitarbeiterInnen innerhalb der sozialen Netze mit ihren Firmen- bzw. Behördenbenutzerkonten zu erfassen, dann wäre dieses Fehlverhalten innerhalb kürzester Zeit aufgefallen und ein möglicher Rufschaden der Organisation hätte verringert werden können.

A.5.1.6 Crossposting

Unter Crossposting bezeichnet man die gleichzeitige Nutzung mehrerer Kanäle, um mit geringem Aufwand einen großen Verbreitungseffekt zu erreichen. Dies kann beispielsweise die Bekanntgabe eines öffentlichen Ereignisses auf Facebook, auf der Webseite der Organisation und auf Twitter sein. Oftmals geschieht dies automatisiert durch RSS Feeds, durch Dienste von Drittanbietern oder Funktionen, die durch das soziale Netz selbst angeboten werden.

Problematisch ist dabei, die Besonderheiten der einzelnen Kanäle zu beachten und zu respektieren. Denn jedes soziale Netz zeichnet sich durch besondere und individuelle Eigenschaften und durch eine spezielle Zielgruppe aus. Deshalb sollte darauf geachtet werden, den auf mehreren sozialen Netzen verteilten Inhalt auf die jeweiligen Eigenschaften und die Zielgruppe der einzelnen Netze anzupassen.

Ein Beispiel für diese Unterschiede ist die erlaubte Länge von Nachrichten, welche in den einzelnen sozialen Netzen sehr unterschiedlich ist. Während auf Facebook und Google+ lange Nachrichten mit mehr als 50.000 Zeichen erlaubt sind, werden Mitteilungen auf Twitter auf 140 Zeichen beschränkt. Wird nun Crossposting zwischen zum Beispiel Facebook und Twitter betrieben, kann durch die Beschränkung der erlaubten Zeichenanzahl möglicherweise nicht der vollständige Inhalt angezeigt werden. Somit wird, nach dem Erreichen der maximalen Zeichenanzahl, der Textfluss unterbrochen und die Nachricht abgeschnitten. Am Ende der gekürzten Nachricht wird ein Link auf Facebook (in folgender Form: "fb.me") angeboten. Folgt man diesem Link, kann es passieren, dass zusätzlich eine Anmeldung bei Facebook erforderlich ist, um den vollständigen Beitrag lesen zu können. Außerdem kann es vorkommen, dass der Zugriff auf die Inhalte aufgrund der Privatsphäreneinstellungen nicht gestattet ist.

Die Länge der Beiträge spiegelt sich auch im allgemeinen Umgangston innerhalb des sozialen Netzes wieder. Während auf Twitter alle Nachrichten sehr gekürzt sind, oftmals im Telegraphen oder SMS Stil verfasst und Links ebenfalls verkürzt werden, sind Nachrichten auf Facebook meist ausführlicher und wenn sinnvoll mit Bildern versehen. Darüber hinaus verfügen viele soziale Netze über Eigenheiten, wie etwa die Hashtags auf Twitter, die nur innerhalb eines bestimmten sozialen Netzes sinnvoll sind.

Dies wissen auch die Benutzer der sozialen Netze und erkennen, wenn eine Organisation oft Crossposting einsetzt. Dadurch kann bei den Benutzern der Eindruck entstehen, dass die Organisation sich nicht auf die individuellen Bedürfnisse der jeweiligen Nutzer einstellt und somit wird der Benutzer auch nicht angesprochen. Im schlimmsten Fall entsteht sogar der Eindruck, die Organisation würde sämtliche zur Verfügung stehenden Kanäle nutzen, um ihre Nachrichten spamartig zu verbreiten.

Besonderer Beachtung beim Crossposting bedarf auch der Rückkanal. Es wird eine eigene Diskussion auf jedem der verwendeten Kanäle geben. Diese Diskussionen gilt es dann alle nach den Vorgaben der Organisation zu bearbeiten.

A.5.2 Risikoassessment

Viele Unternehmen setzen auf soziale Netze, da diese Tools leicht in den Betrieb einzugliedern sind und meist keine Anpassung der IT-Infrastruktur benötigen. Eine Einführung solcher Social-Media-Tools erfolgt oft über den Vorschlag der Marketingabteilung, ohne Einbindung anderer wichtiger Abteilungen, wie der IT, der Projektplanung oder des Risikomanagements. Es ist aber sehr wichtig, dass Unternehmen eine Social-Media-Strategie entwickeln, und einen genau definierten Plan verfolgen, um den Risiken, die diese Technologie mit sich bringt, begegnen zu können.

Auf der einen Seite birgt die Nutzung von sozialen Netzen Risiken, die negative Auswirkungen auf die Unternehmenssicherheit zur Folge haben können. Auf der anderen Seite können sich durchaus Möglichkeiten zum beschleunigten Unternehmenswachstum bieten oder zur Verbesserung des Bekanntheitsgrades des Unternehmens führen. Um den Einfluss von sozialen Netzen auf Unternehmen zu beurteilen, gibt es einige Fragen, die beachtet werden sollten:

- Welche Risiken entstehen durch die Verwendung von sozialen Netzen zur Kommunikation mit Kunden und Geschäftspartnern?
- Welchem Mitarbeiterkreis soll es gestattet werden, Social-Media-Tools im Unternehmensnetzwerk zu benutzen?
- Soll die Nutzung von sozialen Netzen nur für den betrieblichen oder auch für den privaten Gebrauch freigegeben werden?
- Ist es vorgesehen, die Nutzung von sozialen Netzen auf mobilen Endgeräten (Notebooks, Smart Phones, Tablets) zu erlauben?

Ausgehend von diesen Fragen ist es wichtig, bei der Erstellung der Social-Media-Strategie die Risiken und den Nutzen für das Unternehmen gegenüber zu stellen und genau abzuwägen. Hierzu muss eine Risikoanalyse durchgeführt werden, die im Sicherheitshandbuch (s. Kap. 5.1 Risikoanalyse) detailliert beschrieben ist.

Durch die Nutzung von sozialen Netzen ergeben sich zusätzliche Angriffspunkte für Bedrohungen, wie z. B. Malware oder Social Engineering. Die Vielzahl an Bedrohungen in sozialen Netzen beruht auf der Tatsache, dass viele Nutzer Social-Media-Tools verwenden, ohne sich der möglichen Gefahren bewusst zu sein. Daher sollte während der Strategieentwicklung ein Fokus auf das Benutzerverhalten gelegt werden. Darauf aufbauend sollten Richtlinien erstellt werden, die diese Risiken reduzieren, sowie Schulungs- und Sensibilisierungsmaßnahmen für die MitarbeiterInnen ergriffen werden.

Typische Bedrohungen und daraus folgende Risiken im Umgang mit sozialen Netzen werden in Tabelle A.5.1 und Tabelle A.5.2 gezeigt. Tabelle A.5.1 bezieht sich auf Risiken, die im Zusammenhang mit dem Unternehmensauftritt in sozialen Netzen entstehen können. Risiken, welche die private Nutzung von sozialen Netzen mit sich bringen kann, werden in Tabelle A.5.2 angeführt. Für weitere Informationen zu Bedrohungen und der Durchführung einer Bedrohungsanalyse siehe Kapitel 5.1.3.1.4 Bedrohungsanalyse.

Geschäftliche Nutzung von sozialen Netzen im Unternehmen

Bedrohungen/Schwachstellen	Mögliche Risiken	Risikobehandlung
Ausbruch von Malware im Organisationsnetzwerk	• Datenverlust oder -diebstahl • Systemausfälle • Möglicherweise enormer Ressourcenaufwand um Systeme zu bereinigen	• Einsatz von aktueller Anti-Malware-Software auf allen Systemen. (s. Kap. 12.3 Schutz vor Schadprogrammen und Schadfunktionen) • Beschränken von Zugriffsrechten auf soziale Netze. (s. Kap. 9 Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung) • Einführung oder Aktualisierung von Richtlinien. (s. Kap. 4 Informationssicherheitspolitik sowie 18.1.4 Überprüfung auf Einhaltung der Sicherheitspolitiken • Entwicklung und Durchführung von Sensibilisierungsmaßnahmen und -trainings, um die Mitarbeiter über Risiken in sozialen Netzen aufzuklären. (s. Kap. 7.3 Sicherheitssensibilisierung und -schulung)
Belastung der Kunden sowie der Organisation durch betrügerische Handlungen z. B. über gekaperte Benutzerkonten (Social Engineering, Phishing)	• Gefährdung von Kundendaten durch z. B. gezielte Phishing-Attacken auf Kunden oder Mitarbeiter • Rufschädigung	• Entwicklung und Durchführung von Sensibilisierungsmaßnahmen für Kunden, um das Bewusstsein für potenzielle Bedrohungen zu stärken.

Bedrohungen/Schwachstellen	Mögliche Risiken	Risikobehandlung
		• Information der Kunden, welche Informationen diese vom Unternehmen zu erwarten haben.
Unklare bzw. unzureichende Regelungen zur Datennutzung	• Datenverlust • Verlust der Kontrolle über oder Rechten an Informationen, die über soziale Netze kommuniziert werden	• Erarbeitung und Einführung von Richtlinien zur Datennutzung in sozialen Netzen. (Wer darf welche Informationen wann, wie kommunizieren. Siehe Kapitel 8.2 Klassifizierung von Informationen) • Einführung von Protokollierungsmaßnahmen für die Kommunikation in sozialen Netzen, falls möglich. (s. Kap. 12.5 Protokollierung und Monitoring)
Aufwandsanstieg im Kundenservice durch neue Organisationsauftritte in sozialen Netzen	• Verschlechterung der Kundenzufriedenheit • Mögliche Rufschädigung oder negative Auswirkung auf Kundenbindung	• Sicherzustellen ist, dass ausreichend Personalressourcen zur Bewältigung der Serviceanfragen vorhanden sind. • Erstellen von eigenen Bereichen für Kundenanfragen im sozialen Netz, falls möglich.

Tabelle A.5.1: Bedrohungen/Schwachstellen, Risiken und Risikobehandlung bei geschäftlicher Nutzung von sozialen Netzen (Quelle: nach ISACA: Social Media: Business Benefits and Security, Governance and Assurance Perspectives (2010), Seite 7.)

Private Nutzung von sozialen Netzen im Unternehmen

Bedrohungen/Schwachstellen	Mögliche Risiken	Risikobehandlung
Nutzung von persönlichen Benutzerkonten in sozialen Netzen, um geschäftliche Informationen zu kommunizieren	• Rufschädigung • Möglicher Verlust von Wettbewerbsvorteilen • Verstoß gegen Datenschutz oder Geheimhaltungsverpflichtungen	• Erstellen von Richtlinien zur Datennutzung in sozialen Netzen, um sicherzustellen, welche organisationsbezogenen Informationen kommuniziert werden dürfen. • Erarbeitung und Durchführung von Sensibilisierungsmaßnahmen und -trainings zur Stärkung dieser Richtlinien.

Bedrohungen/Schwachstellen	Mögliche Risiken	Risikobehandlung
Kommunikation von Informationen (z. B. Bilder, Organisationslogos) durch Mitarbeiter, die Rückschlüsse auf die Organisation zulassen	• Mögliche Ruf- oder Markenschädigung	• Erarbeiten von Regelungen, wie Mitarbeiter im Zusammenhang mit ihren Auftritten in sozialen Netzen organisationsspezifischen Informationen (wie z. B. Logos, Vermögenswerte, geistiges Eigentum) verwenden dürfen. • Definieren eines Prozesses zur Freigabe von organisations-spezifischen Informationen.
Übermäßige persönliche Nutzung von sozialen Netzen am Arbeitsplatz	• Möglicherweise erhöhte Netzwerkauslastung • Produktivitätsverlust • Erhöhtes Malware-Risiko	• Einsatz von Systemen zur Inhaltsfilterung, um den Zugang zu sozialen Netzen zu verwalten, falls möglich. • Begrenzung des Datendurchsatzes im Netzwerk zu sozialen Netzen, falls möglich.
Nutzung von sozialen Netzen auf organisationsinternen mobilen Endgeräten (Smartphones, Tablets, Notebooks)	• Erhöhtes Malware-Risiko auf mobilen Endgeräten • Möglicher Datenverlust oder Datendiebstahl • Umgehung von organisationsinternen Kontrollmechanismen	• Wenn möglich, sollte der Zugriff auf soziale Netze auf mobilen Endgeräten beschränkt werden. • Einsatz von aktueller Anti-Malware bzw. Kontrollsoftware auf mobilen Endgeräten. • Erarbeiten oder Aktualisieren von Richtlinien, um die Nutzung von sozialen Netzen auf mobilen Endgeräten zu definieren. • Erstellung und Durchführung von Sensibilisierungsmaßnahmen und -trainings, um das Bewusstsein der Mitarbeiter über etwaige Risiken, die durch die Nutzung von sozialen Netzen auf mobilen Endgeräten bestehen, zu stärken.

Tabelle A.5.2: Bedrohungen/Schwachstellen, Risiken und Risikobehandlung bei privater Nutzung von sozialen Netzen (Quelle: nach ISACA: Social Media: Business Benefits and Security, Governance and Assurance Perspectives (2010), Seite 8.)

A.5.3 Sicherheitseinstellungen und Umgang mit sozialen Netzen

Die MitarbeiterInnen, die soziale Netze beruflich nutzen, müssen die Vorgaben zum Verhalten in sozialen Netzen (Social Media Guidelines) einhalten. Dazu gehören zum einen die Umsetzung von IT-sicherheitsrelevanten Einstellungen, die vom sozialen Netz angeboten werden und zum anderen der richtige Umgang mit sozialen Netzen. Hierzu ist es wichtig, dass diese MitarbeiterInnen regelmäßig geschult werden, um auf aktuelle Gegebenheiten effektiv reagieren zu können.

Des Weiteren sollten Sicherheitseinstellungen, die vom sozialen Netz angeboten werden, bekannt sein und ihre Anwendung in einer sinnvollen und aktuellen Richtlinie vorgeschrieben werden. Eine regelmäßige Überprüfung und Anpassung dieser Richtline wird empfohlen, da soziale Netze dazu tendieren, die angebotenen Sicherheitseinstellungen sowohl in ihrer Menüstruktur als auch inhaltlich mehrfach zu verändern.

Im Folgenden werden einige Einstellungsmöglichkeiten dargestellt. Sie sind als Beispiel gedacht und sollten keinesfalls ohne Prüfung und Anpassung an die für die eigene Organisation bestehenden Anforderungen angewandt werden.

A.5.3.1 Facebook

Unterschiedliche Sichtbarkeit von Beiträgen in Facebook:

Zur Bestimmung der Sichtbarkeit von Beiträgen empfiehlt sich die Verwendung von Listen (diese können mit der Funktion „Freundeslisten“ angelegt und verwaltet werden). Für ein berufliches Profil kann beispielsweise eine Liste für alle Kontakte innerhalb der eigenen Organisation angelegt werden und eine andere Liste für Kontakte anderer Organisationen. Denkbar sind auch Listen für einzelne Abteilungen innerhalb der eigenen Organisation. In den Privatsphäre-Einstellungen sollte die Option für „Wer kann deine zukünftigen Beiträge sehen?“ auf einen ungefährlichen Standardwert gestellt werden. Beispielsweise auf eine Liste „Meine Organisation“ (Abb. A.5.1). Dies verhindert ein versehentliches Veröffentlichen von Informationen an Dritte. Wenn Beiträge geschrieben werden, die nicht für die voreingestellte Liste gedacht sind, muss die Sichtbarkeit beim entsprechenden Beitrag geändert werden.

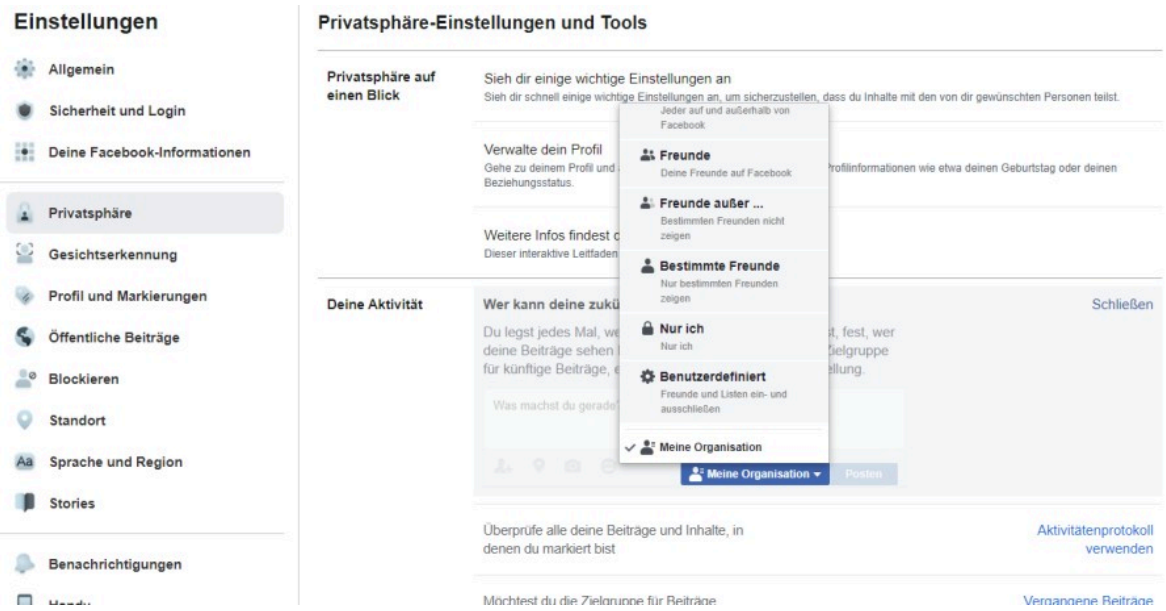

Abbildung A.5.1: Facebook 2020. Privatsphäre-Einstellungen: Sichtbarkeit der eigenen Inhalte in Facebook.

Beiträge in Facebook, in denen das eigene Profil von Freunden markiert wird:

In Facebook ist das Markieren von Profilen in Beiträgen eine mächtige Funktion. Es entsteht nicht nur eine einfache Verlinkung des Profils mit dem Beitrag, sondern jedes markierte Profil kann den Beitrag, in dem es markiert wurde, sehen – ungeachtet der sonstigen Privatsphäre-Einstellungen für diesen Beitrag. Ein Profil, das beispielsweise für den öffentlichen Auftritt einer Organisation in Facebook verwendet wird, und Kunden als Freunde in Facebook sammelt, beispielsweise zum Zweck von Kundenbindung, kann Markierungen von Kunden z. B. für Marketingzwecke zulassen. Um einige in diesem Zusammenhang typische Gefährdungen aufzuzeigen, folgen zwei beispielhafte Szenarien.

Szenario 1:
Ein Kunde kauft ein neues Auto zu günstigen Konditionen und stellt stolz ein Bild seines Fahrzeugs auf Facebook, zusammen mit einer kurzen Geschichte über den vorteilhaften Ratenkauf. Auf diesem Bild markiert er das öffentliche Profil des Autohauses, bei dem er das Fahrzeug erstanden hat. Standardmäßig erscheint der Beitrag nun in der Chronik des öffentlichen Profils des Autohauses, das in dem Beitrag des Kunden markiert wurde, sowie in der Chronik des Kunden, der den Beitrag verfasst hat.

Szenario 2:

Ein anderer Kunde kauft einen Gebrauchtwagen und touchiert beim Verlassen des Parkplatzes des Autohauses eine Mauer. Er verlangt vom Autohausbetreiber eine Beteiligung an der Reparatur. Der Autohändler erklärt, dass der Kunde die Verantwortung für das Fahrzeug übernommen hat, als er mit den Schlüsseln eingestiegen und losgefahren ist und somit die Reparaturkosten vom Kunden zu tragen sind. Zuhause angelangt, beginnt der Kunde verärgert das öffentliche Profil des Autohauses auf Bildern mit schrottreifen Fahrzeugen in Facebook zu markieren und darunter anstößige Texte zu verfassen. Standardmäßig erscheinen nun diese Beiträge ebenfalls in der Chronik des öffentlichen Profils des Autohauses.

Um derartige Szenarien zu verhindern gibt es zwei Möglichkeiten. Entweder, Freundschaftsanfragen auf Facebook von Kunden dürfen nicht angenommen werden, so dass kein Kunde die Möglichkeit hat das öffentliche Profil der Organisation in Beiträgen zu markieren, oder alle Beiträge, in denen das Profil markiert wird, müssen von einem zuständigen Mitarbeiter geprüft werden, bevor sie in der Chronik des eigenen Profils erscheinen (Abb. A.5/2). Die zweite Möglichkeit verhindert nicht, dass Beiträge mit Markierungen des eigenen Profils in der Chronik des Benutzers erscheinen, der das Profil markiert.

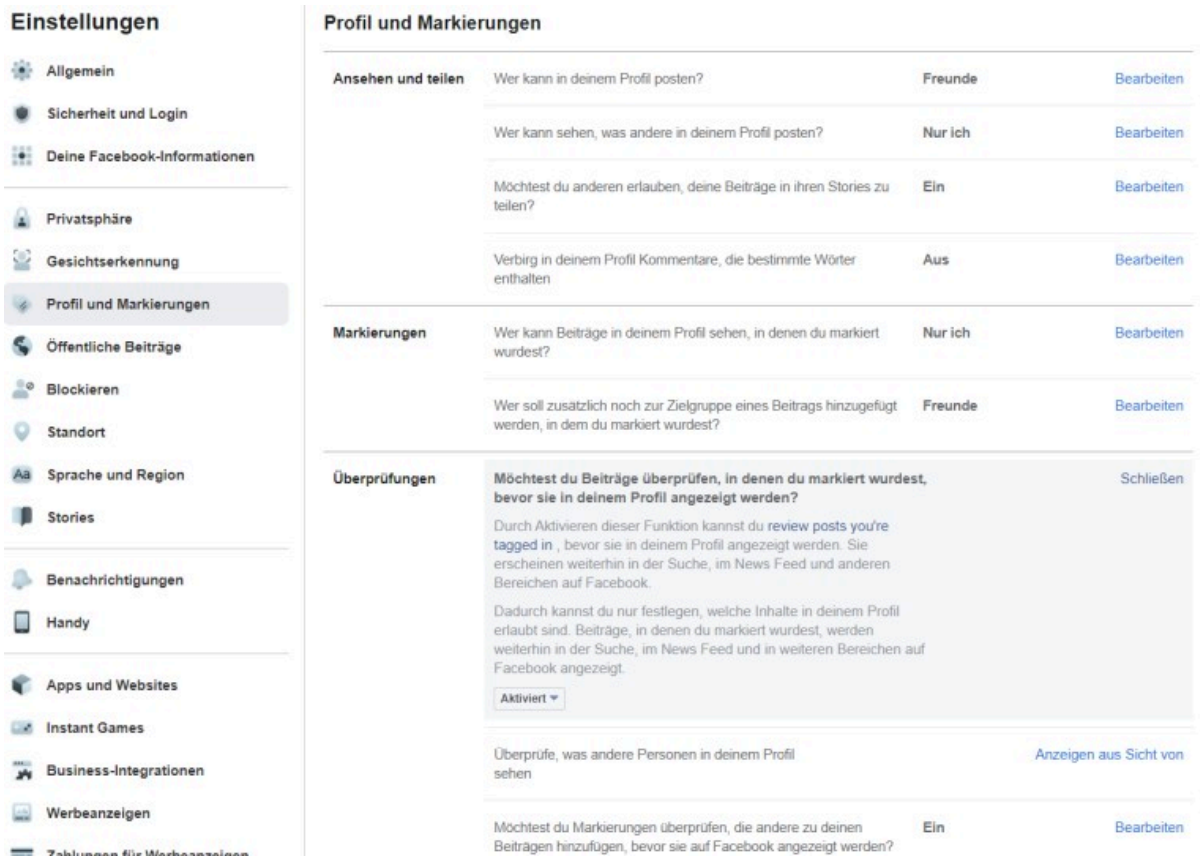

Abbildung A.5.2: Facebook 2020. Profil und Markierungseinstellungen: Prüfen von Beiträgen, auf denen das eigene Profil markiert wurde, bevor sie im eigenen Profil erscheinen.

Zusätzlich zu den Sicherheitseinstellungen in sozialen Netzen, ist der richtige Umgang der MitarbeiterInnen mit sozialen Netzen für ein Unternehmen oder eine Behörde von essentieller Bedeutung. Das nachfolgende Szenario soll mögliche Auswirkungen privater Nutzung von sozialen Netzen im Behördenumfeld beispielhaft veranschaulichen. Eine detaillierte Maßnahmenbeschreibung zum Umgang mit sozialen Netzen ist im dokumentinternen Kapitel A.5.4.2 Maßnahmen zum Umgang mit sozialen Netzen enthalten.

Szenario 3:
Angenommen ein Mitarbeiter einer Behörde verwendet in seiner privaten Zeit und mit seinem privaten Account ein soziales Netz. In diesem sozialen Netz ist er mit einer Mitarbeiterin eines IT-Systemhauses befreundet. Sie hilft ihm zeitweise bei privaten IT-Fragen mit ihrem Wissen aus. Dabei verlaufen Gespräche auch über Möglichkeiten gewisse Softwareprodukte im Arbeitsplatzumfeld zu verwenden. Aufgrund des durch die Mitarbeiterin gewonnenen guten Eindrucks des IT-Systemhauses klickte der Mitarbeiter der Behörde bereits vor längerer Zeit auf die Like-Funktion auf dem öffentlichen Profil des IT-Systemhauses.

Bei der nächsten öffentlichen Ausschreibung der Behörde für ein neues Softwareprodukt beteiligt sich auch das oben genannte IT-Systemhaus als Bieter. Sollte der Zuschlag der Ausschreibung auf das IT-Systemhaus fallen, so könnten Mitbewerber ein Naheverhältnis zwischen dem Mitarbeiter der Behörde, und dem IT-Systemhaus vermuten, aufgrund des privaten Kontaktes zwischen dem Mitarbeiter der Behörde und der Mitarbeiterin des IT-Systemhauses. Insbesondere die Like-Funktion kann hierbei problematisch sein.

Informationen über private Kontakte zwischen Angestellten von Firmen und MitarbeiterInnen von Behörden werden oftmals erst durch soziale Netze der Öffentlichkeit zugänglich. Je nach verwendetem sozialem Netz sind diese Informationen auch nur schwer bis gar nicht wieder zu entfernen.

A.5.3.2 Xing und LinkedIn

Die sozialen Netzwerke Xing und LinkedIn werden häufig auch für berufliches Netzwerken bzw. auch für Profile von Unternehmen bzw. Organisationen genutzt. Den MitarbeiterInnen sollte bewusst sein, welche Informationen öffentlich auffindbar sind und wie sie die Sichtbarkeit von Informationen einschränken können (bei Xing unter Einstellungen -> Privatsphäre, siehe Abb. A.5/3; bei LinkedIn unter Einstellungen & Datenschutz -> Sichtbarkeit, siehe Abb. A.5/4 bzw. Einstellungen & Datenschutz -> Datenschutz, siehe Abb. A.5/5).

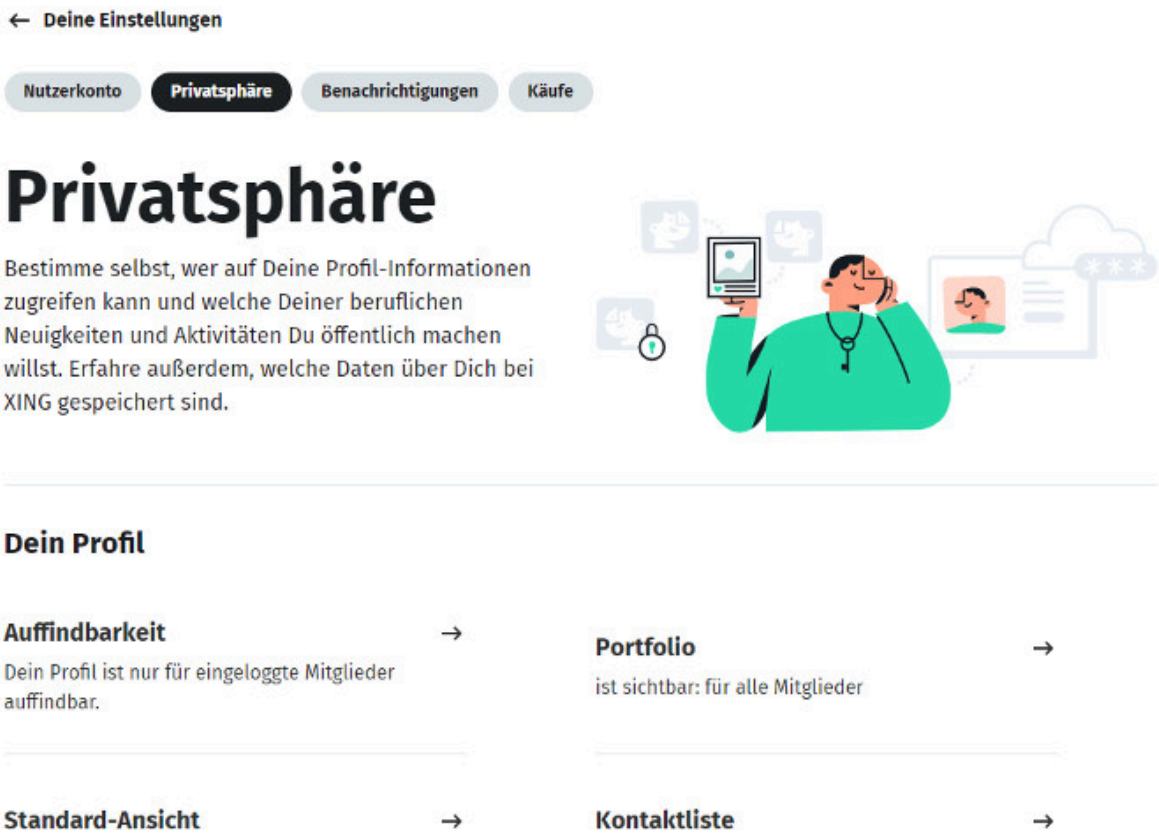

Abbildung A.5.3: Xing 2020. Privatsphäre Einstellungen

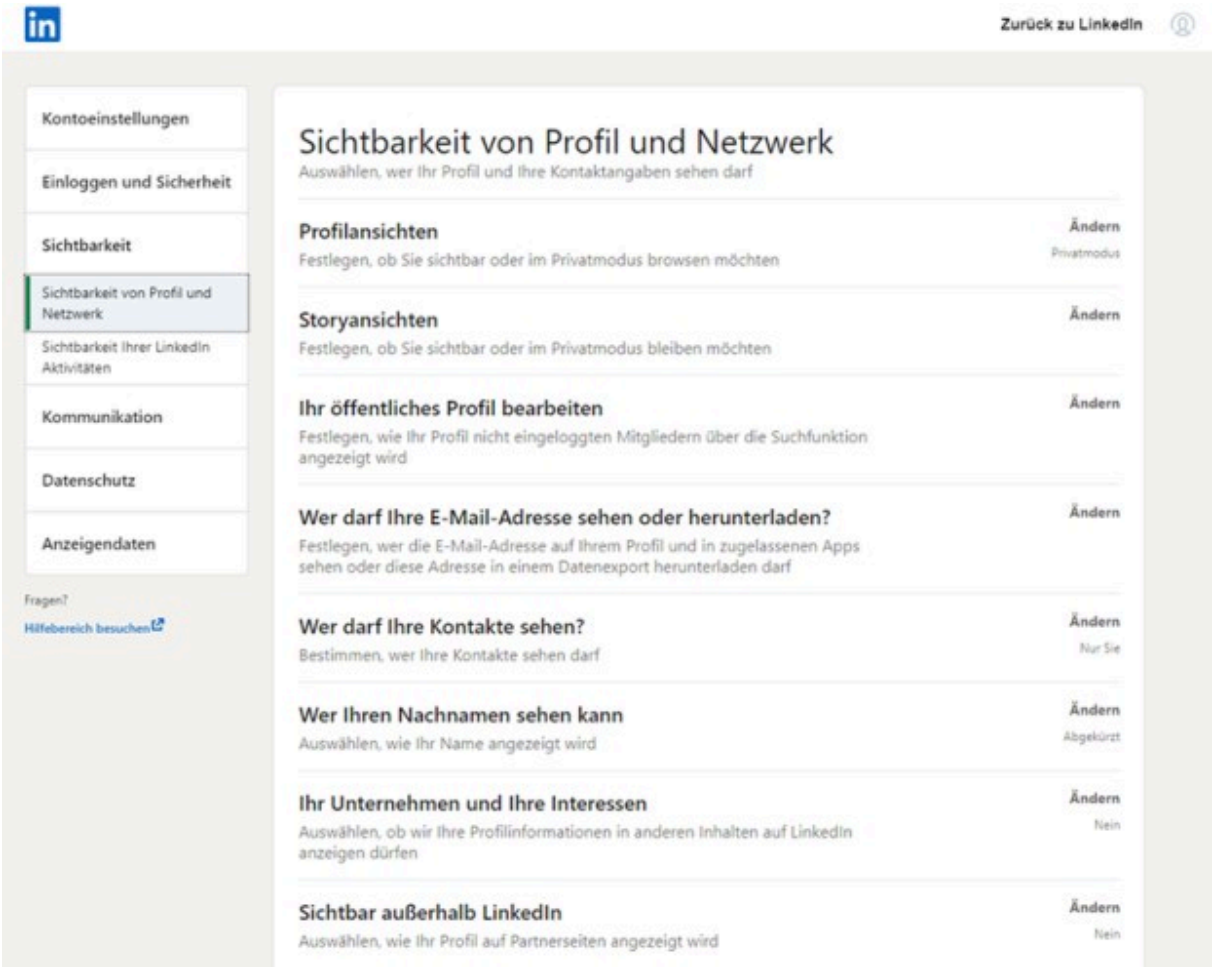

Abbildung A.5.4: LinkedIn 2020: Einstellungen zur Sichtbarkeit von Profil und Netzwerk

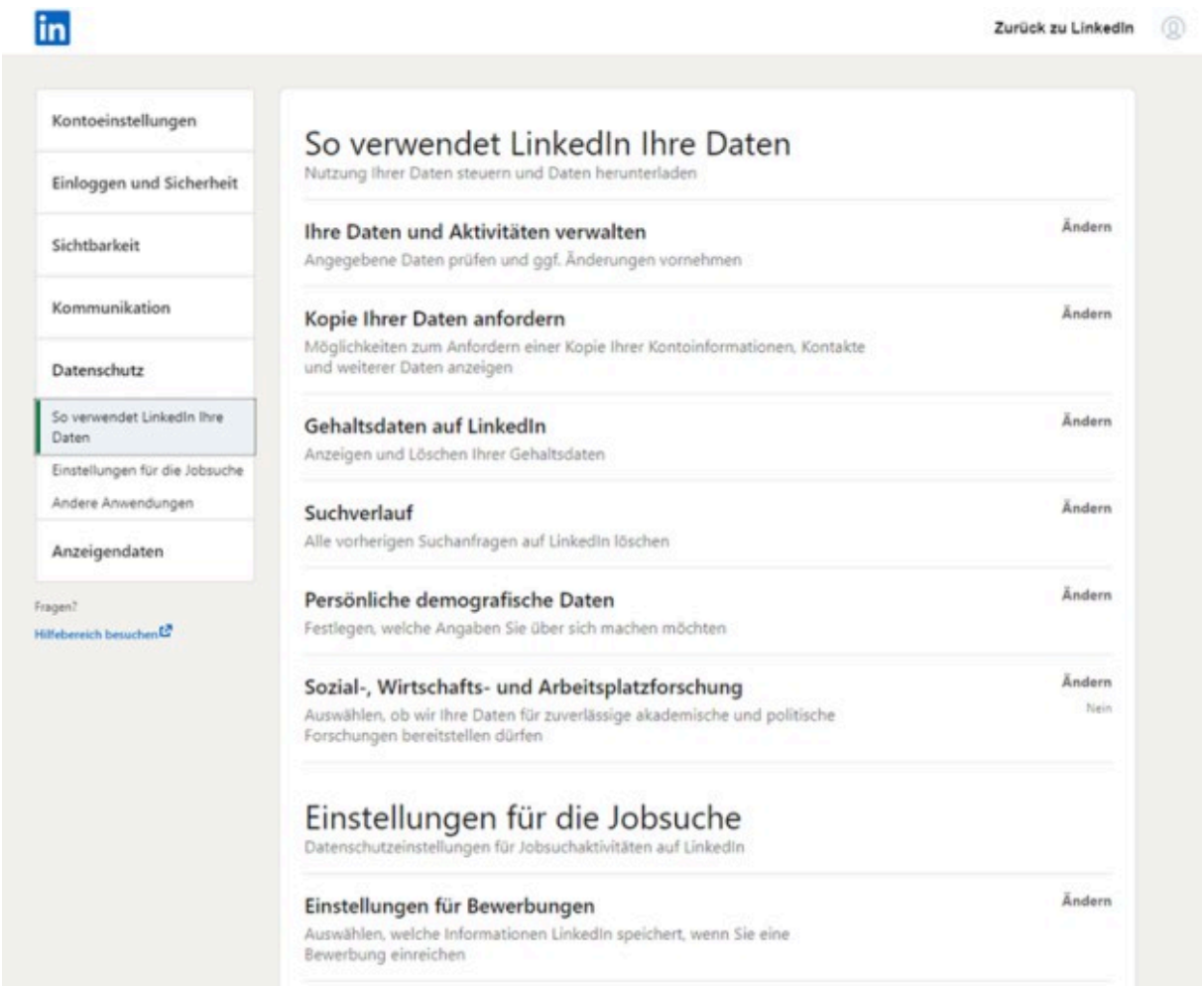

Abbildung A.5.5: LinkedIn 2020: Einstellungen zu Datenschutz

A.5.3.3 Schritt-für-Schritt-Anleitungen

Aktuelle Schritt-für-Schritt Anleitungen und weitere wichtige Informationen zu verschiedenen ausgewählten Sozialen Netzwerken (WhatsApp, Instagram, Snapchat, Facebook, Facebook Messenger, TikTok, Google, YouTube) sind in den Privatsphäre-Leitfäden von Saferinternet.at verfügbar, die regelmäßig aktualisiert werden.

A.5.4 Richtlinie zur Sicherheit in sozialen Netzen

Um die Nutzung von sozialen Netzen effektiv zu steuern ist es erforderlich, eine dokumentierte Strategie und ein klar definiertes Regelwerk zu entwickeln. In den Entwicklungs- und Erstellungsprozess dieser strategischen Richtlinie sollten alle relevanten Stakeholder eingebunden werden. Dazu zählen zum Beispiel:

- die Leitungsebene,
- das Risikomanagement,

- die Personalabteilung,
- die Rechtsabteilung,
- die Presse- und Öffentlichkeitsarbeit, sowie
- die IT-Abteilung.

In der Richtlinie zur Sicherheit in sozialen Netzen – in der Literatur oftmals als Social Media Guidelines bezeichnet – sollte genau definiert sein, wie die Kommunikation in sozialen Netzen abzulaufen hat und welche Informationen freigegeben werden. Des Weiteren sollten insbesondere folgende Punkte enthalten sein:

- Definition der Verantwortlichkeiten,
- Vorgaben zu den Sicherheitsmaßnahmen (z. B. die Sicherheitseinstellungen der Accounts),
- Vorgaben über die Vorgehensweise beim Auftreten von Sicherheitsvorfällen (z. B. Datenlecks, Social Engineering),
- Festlegung der Datennutzung,
- Vorgaben an den Benutzer zur Handhabung von sozialen Netzen,
- Regelungen zur Schulung und Sensibilisierung von MitarbeiterInnen (Verhaltensregeln in sozialen Netzen),
- die Gültigkeit der Richtlinie, sowie
- mögliche Sanktionen bei Nichteinhaltung der Regelungen.

Für weitere Anhaltspunkte zum Erstellen einer geeigneten Richtlinie siehe Kapitel 4 Informationssicherheitspolitik und Kapitel 13.2.1 Richtlinien beim Datenaustausch mit Dritten.

A.5.4.1 Verantwortlichkeiten

In diesem Abschnitt werden die Zuständigkeiten in Bezug auf die Sicherheit in sozialen Netzen definiert. Zu den Aufgaben des Sicherheitsverantwortlichen für Soziale Netze sollten folgende Punkte zählen:

- die Planung und Umsetzung von Sicherheitsmaßnahmen in sozialen Netzen,
- die Prüfung der Einhaltung dieser Maßnahmen,
- die Reaktion auf sicherheitsrelevante Ereignisse, sowie
- die Planung und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen.

Diese Anforderungen können beispielsweise durch den/die in Kapitel 6.1.3.3 Der/Die Informationssicherheitskoordinator/in im Bereich beschriebenen Informationssicherheitskoordinator/in im Bereich wahrgenommen werden. Detaillierte Informationen zum Thema Organisation und Verantwortlichkeiten im Informationssicherheitsprozess sind in Kapitel 6.1.3 Organisation und Verantwortlichkeiten für Informationssicherheit enthalten.

A.5.4.2 Maßnahmen zum Umgang mit sozialen Netzen

Zur wirkungsvollen Steuerung des Umgangs mit sozialen Netzen sollte die Richtlinie sowohl den betrieblichen bzw. dienstlichen als auch den privaten Umgang in der Organisation regeln. Hierzu sollen für Unternehmen insbesondere folgende Bereiche abgedeckt werden:

Die private Nutzung von sozialen Netzen im Unternehmensumfeld:

- Klarstellung, ob bzw. in welchem Umfang eine private Nutzung von sozialen Netzen am Arbeitsplatz erlaubt wird und falls ja, ob dies auch auf Firmeneigentum gestattet wird.
- Regelungen zur Nutzung von geschäftlichen E-Mail-Adressen und Signaturen sind zu definieren.
- Die Geheimhaltungsverpflichtungen sind einzuhalten.
- Es ist sicherzustellen, dass alle gesetzlichen Vorgaben eingehalten werden – besondere Beachtung ist dabei auf das Datenschutzgesetz, Copyright und Urheberrecht zu legen.
- Vorgaben zur Regelung von unternehmensbezogenen Postings oder Diskussionen sind zu definieren. Es muss sichergestellt werden, dass bei der privaten Nutzung von sozialen Netzen der Nutzer nicht als Repräsentant des Unternehmens auftritt.
- Postings, die den Ruf des Unternehmens schädigen könnten, sind zu vermeiden.
- Diskussionen zwischen Arbeitskollegen über firmenbezogene Inhalte dürfen nur über firmeninterne Kanäle erfolgen (z. B. Intranet, interne E-Mails).
- Zwischen Kollegen entstandene Meinungsverschiedenheiten dürfen nicht auf öffentlichen Kanälen diskutiert werden.

Die Nutzung für geschäftliche Zwecke im Unternehmensumfeld:

- Klarstellung, ob bzw. in welchem Umfang die geschäftliche oder dienstliche Nutzung erlaubt wird (z. B. Freigabe nur auf Firmeneigentum oder auch auf privaten Geräten).
- Zugriffsrechte sind zu definieren.

- Vorgaben zur Regelung von unternehmensbezogenen Postings oder Diskussionen sind zu definieren, um sicherzustellen, dass geltende Zuständigkeitsbereiche und Berechtigungen eingehalten werden.
- Es müssen Vorgaben zur Datennutzung erstellt werden.
- Postings von MitarbeiterInnen sollten immer Rückschlüsse auf die Position innerhalb des Unternehmens bzw. der Abteilung zulassen.
- Veröffentlichte Informationen müssen auf dem aktuellen Stand gehalten und etwaige Fehler (z. B. Falschmeldungen, Rechtschreibfehler) korrigiert werden.
- Regelungen bzw. Verbote zum Aufruf unangemessener Webseiten, Inhalte (rassistische, pornografische und verbotene Inhalte), sowie zu nicht gestatteten Aktivitäten müssen definiert werden (z. B. Installation von Plug-Ins, Spielen).
- Profile sollten nur die nötigsten privaten Daten enthalten.
- Ein Eskalationsprozess für Kundenprobleme muss definiert werden.
- Monitoring Prozesse und Prozesse zum Markenschutz müssen erstellt werden.
- MitarbeiterInnen sind für den geschäftlichen Umgang mit sozialen Netzen so zu schulen, dass sie die vom Unternehmen vorgegebenen Regeln verstehen und umsetzen können

Für Behörden sollen insbesondere folgende Bereiche abgedeckt werden:

Die private Nutzung von sozialen Netzen im Behördenumfeld:

- Klarstellung, ob bzw. in welchem Umfang eine private Nutzung von sozialen Netzen am Arbeitsplatz erlaubt wird und falls ja, ob dies auch von dienstlichen Geräten gestattet wird.
- Regelungen zur Nutzung von dienstlichen E-Mail-Adressen und Signaturen sind zu definieren.
- Sind Informationen auf einem privaten Account enthalten, die eine Verbindung zu der Behörde zulassen, so gilt die Nutzung nicht mehr als rein privat.
- Die Geheimhaltungsverpflichtungen sowie die Amtsverschwiegenheit und die Dienstordnung sind einzuhalten.
- Vorgaben zur Regelung von behördenbezogenen Postings oder Diskussionen sind zu definieren. Es muss sichergestellt werden, dass bei der privaten Nutzung von sozialen Netzen der Nutzer nicht als Repräsentant der Behörde auftritt.
- Postings, die den Ruf der Behörde schädigen könnten, sind zu vermeiden.
- Diskussionen zu behördenbezogenen Inhalten dürfen nur über behördeninterne Kanäle erfolgen (z. B. Intranet, interne E-Mails).
- Zwischen Kollegen entstandene Meinungsverschiedenheiten dürfen nicht auf öffentlichen Kanälen diskutiert werden.

Die Nutzung für dienstliche Zwecke im Behördenumfeld:

- Bedingungen zur Nutzung von sozialen Netzen sind zu erstellen bzw. bestehende Nutzungsbedingungen oder bundes- und länderspezifische Erlässe sind zu befolgen.
- Klarstellung, ob bzw. in welchem Umfang die dienstliche Nutzung erlaubt wird (z. B. Freigabe nur auf dienstlichen oder auch auf privaten Geräten).
- Zugriffsrechte sind zu definieren.
- Vorgaben zur Regelung von behördenbezogenen Postings oder Diskussionen sind zu definieren, um sicherzustellen, dass geltende Zuständigkeitsbereiche und Berechtigungen eingehalten werden.
- Es müssen Vorgaben zur Datennutzung erstellt werden.
- Die Geheimhaltungsverpflichtungen sowie die Amtsverschwiegenheit und die Dienstordnung sind einzuhalten.
- Postings von MitarbeiterInnen sollten immer Rückschlüsse auf die Position innerhalb der Behörde bzw. der Abteilung zulassen und politisch neutral formuliert sein.
- Veröffentlichte Informationen müssen auf dem aktuellen Stand gehalten und etwaige Fehler (z. B. Falschmeldungen, Rechtschreibfehler) korrigiert werden.
- Regelungen bzw. Verbote zum Aufruf unangemessener Webseiten, Inhalte (rassistische, pornografische und verbotene Inhalte), sowie zu nicht gestatteten Aktivitäten müssen definiert werden (z. B. Installation von Plug-Ins, Spielen).
- Profile sollten nur die nötigsten privaten Daten enthalten.
- Monitoring Prozesse und Prozesse zum Markenschutzmüssen erstellt werden.
- MitarbeiterInnen sind für den dienstlichen Umgang mit sozialen Netzen so zu schulen, dass sie die von der Behörde vorgegebenen Regeln verstehen und umsetzen können.

Besonderer Beachtung bedürfen die zu verarbeitenden Informationen bei der geschäftlichen bzw. dienstlichen Nutzung von sozialen Netzen. Es gilt es genaue Regelungen zu erstellen, welche Informationen über soziale Netze kommuniziert werden dürfen.

Zusätzlich sollte darauf geachtet werden keine klassifizierten Informationen, die in Kapitel 8.2 Klassifizierung von Informationen erläutert werden, zu veröffentlichen.

A.5.4.3 Anforderungen an den Benutzer

Die Verwendung von sozialen Netzen im beruflichen Umfeld fordert Vorbereitung und Schulung der betroffenen MitarbeiterInnen einer Organisation. Die MitarbeiterInnen müssen sich bewusst sein, dass sie ihre Organisation nach außen hin vertreten.

A.5.4.3.1 Abmelden des Nutzers / Bildschirmsperre

Der Nutzer ist verpflichtet, sich vom verwendeten Dienst abzumelden, bzw. seinen Bildschirm zu sperren, sobald er sich vom Arbeitsplatz entfernt. Siehe Kapitel 7.1.9 Verpflichtung der PC-BenutzerInnen zum Abmelden.

A.5.4.3.2 Passwort Policy

Die Wahl eines geeigneten Passwortes für die Nutzung des sozialen Netzes muss nach der aktuellen Passwort Policy erfolgen. Siehe Kapitel 9.3 Verantwortung der BenutzerInnen.

A.5.4.4 Incident Handling

Die Reaktion auf Sicherheitsvorfälle bzw. sicherheitsrelevante Ereignisse muss so schnell und effektiv wie möglich geschehen. Dazu müssen geeignete Vorgehensweisen sowie Organisationsstrukturen existieren und den MitarbeiterInnen bekannt sein. Die Behandlung von Sicherheitsereignissen muss auch im Sicherheitskonzept der Organisation beschrieben sein. Insbesondere muss sichergestellt werden, dass Sicherheitsvorfälle bzw. sicherheitsrelevante Ereignisse von den MitarbeiterInnen umgehend auf dem dafür vorgesehenen Meldeweg gemeldet werden. Für eine detaillierte Beschreibung von Incident Handling siehe Kapitel 16.1 Reaktion auf Sicherheitsvorfälle bzw. sicherheitsrelevante Ereignisse (Incident Handling).

A.5.4.5 Awarenessbildende Maßnahmen

Ein professioneller und erfolgreicher Auftritt eines Unternehmens oder einer Behörde in sozialen Netzen setzt voraus, dass auch jeder Mitarbeiter, der beruflich mit sozialen Netzen in Kontakt kommt, professionell auftritt. Um dies zu unterstützen sind hinreichende und regelmäßige Mitarbeiterschulungen unabdingbar. Der Umgang mit den Kontakten außerhalb der eigenen Organisation im sozialen Netz will gelernt sein, insbesondere wenn es einmal zu unerwünschten Reaktionen seitens der Zielgruppe kommt. Hinzu kommen Änderungen und Ergänzungen bei aktuellen Sicherheitseinstellungen, die vom sozialen Netz angeboten werden, die den Mitarbeitern zeitnah erläutert werden sollen. Des Weiteren ist ein Awareness-Training für die Erkennung und das Reagieren auf Social Engineering Angriffe, gerade auch im Bereich soziale Netze, unverzichtbar.

Damit sich die MitarbeiterInnen sicher in sozialen Netzen bewegen können, müssen diese über mögliche Bedrohungen und Gefahren aufgeklärt werden. Sichergestellt werden kann dies über eine speziell auf soziale Netze abgestimmte Security Awareness Kampagne. Diese trägt maßgeblich zu einer Bewusstseinsförderung

der MitarbeiterInnen bei und kann somit die Eintrittswahrscheinlichkeit eines Sicherheitsvorfalles mindern. Um eine möglichst starke Sensibilisierung der MitarbeiterInnen zu erzielen, sollten die Security Awareness Maßnahmen sowie die Verhaltensregeln für soziale Netze folgende Punkte enthalten:

- Der richtige Umgang mit den Privatsphäre-Einstellungen der einzelnen sozialen Netze,
- Einhaltung der geltenden Gesetze und betriebsinternen Vorschriften,
- Kenntnis der jeweiligen Allgemeinen Geschäftsbedingungen der sozialen Netze,
- Trennung zwischen Beruflichem und Privatem,
- eine sachliche und professionelle Kommunikation (z. B. Vermeidung von Beleidigungen und negativen Äußerungen über Mitbewerber oder deren Produkte),
- Umgang mit geschäftsschädigenden oder missverständlichen Inhalten (z. B. Wann dürfen Postings gelöscht werden?),
- Verwendung von sicheren und unterschiedlichen Passwörtern für die verschiedenen sozialen Netze,
- Schutz gegen Schadsoftware,
- Aufklärung der MitarbeiterInnen über aktuelle Bedrohungen in sozialen Netzen, wie zum Beispiel Phishing, Social Engineering oder Identity Theft sowie
- Aufklärung der MitarbeiterInnen über typische Schwachstellen, die ein Angreifer ausnutzen könnte. Beispiele hierfür sind:
    - unsicheres Passwortmanagement,
    - die Nutzung von identischen Passwörtern für unterschiedliche soziale Netze,
    - Sicherheitsrisiken, die bei der Nutzung von unsicheren oder nicht vertrauenswürdigen Applikationen von Drittanbietern – vor allem auf mobilen Endgeräten – entstehen,
    - durch die laufende Aktualisierung der sozialen Netze können sich unbemerkte Änderungen in den Privatsphäre-Einstellungen ergeben sowie
    - mangelnde Kenntnisse der MitarbeiterInnen im Umgang mit sozialen Netzen und ein geringes Bewusstsein für vorhandene Gefahren und Bedrohungen – wie zum Beispiel das Erkennen von Social Engineering Angriffen.

Social Engineering ist ein ernst zu nehmendes Thema, insbesondere auch im Bereich sozialer Netze, da Mitarbeiter oft dazu neigen, dort einen etwas lockereren Umgang zu pflegen. Um einen möglichen Social Engineering Angriff zu erschweren, sollten regelmäßig spezielle Awareness-Trainings stattfinden (z. B. Social Engineering Workshops).

Die Reaktion auf unerwünschte Einträge muss in die Verhaltensregeln Einzug finden. Dabei sollte geklärt werden, bis zu welchen Grenzen eine Diskussion geführt wird und ab wann ein Eintrag (kommentarlos) zu löschen ist. Hier sollte beachtet werden, dass eine Löschung des Eintrages zwar zunächst als eine einfache und schnelle Lösung erscheint, aber mit Bedacht gewählt werden sollte, um nicht Gefahr zu laufen der Zensur beschuldigt zu werden. Viele Nutzer sozialer Netze sehen die Löschung eines Eintrages sehr negativ. Bei verbalen Angriffen und/oder Belästigungen sollte ein Eintrag allerdings gelöscht werden. Handelt es sich um konstruktive Kritik, sollte ein Beitrag jedoch nicht kommentarlos entfernt werden. Generell sollte darauf geachtet werden, dass die Social Media Guidelines keine zu strikten Kommunikationsregeln enthalten, um eine dynamische Entwicklung, wie sie in sozialen Netzen aufkommt, zu unterstützen.

Für weitere Informationen zu Security Awareness und Schulungen siehe Kapitel 2.3.2 Sensibilisierung (Security Awareness), Kapitel 2.3.3 Schulung und Kapitel 3.2.2 Schulung und Awareness.

A.5.4.6 Geltungsbereich

Generell ist ein Geltungsbereich für Richtlinien durch das Management zu definieren. Hierbei gilt es genau abzugrenzen, für welche Bereiche die Richtlinie Gültigkeit besitzt und an welche Bereiche die Richtlinie kommuniziert werden soll (z. B. MitarbeiterInnen, Kunden, Service-Dienstleister oder Partnerorganisationen).
Alle, die die von der Organisation erarbeitete Richtlinie zur Sicherheit mit sozialen Netzen betrifft, sind verpflichtet, sich an die in der Richtlinie enthaltenen Vorgaben der Organisation sowie an einschlägige Gesetze zu halten. Dies ist seitens der Organisation zu prüfen nach Kapitel 7.1.10 Kontrolle der Einhaltung der organisatorischen Vorgaben. Die Richtlinie tritt mit der Freigabe durch das Management in Kraft. Es gilt die jeweils aktuelle Fassung bis auf Widerruf. Detaillierte Informationen sind in Kapitel 7.1.1 Verpflichtung der MitarbeiterInnen zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen zu finden.

A.6 Sichere Beschaffung

Sinngemäß muss nach Abschnitt 6.1.5 des Informationssicherheitshandbuchs die Beschaffung, die Installation und der Betrieb von informationsverarbeitenden Komponenten aller Art koordiniert und genehmigt werden. Dies betrifft die geregelte Abnahme, die Freigabe, die Installation und die Benutzung von Komponenten wie auch etwa externen Laufwerke, USB-Sticks, PDAs, Smartphones, Tablet-Computer und die darauf installierte Software (z.B.: Betriebssystem, Apps).

Um mögliche Risiken im Bereich von internen oder externen Beschaffungs- bzw. Vergabevorgängen mit IT-Sicherheitsaspekten zu reduzieren, sind das Zusammenwirken der beteiligten Akteure gemeinsam mit der methodischen Anwendung von sicheren Beschaffungsprinzipien und das kontinuierliche Management der bestehenden Wirkungsbeziehungen unerlässlich. Damit ist die Anschaffung komplexer, vertrauenswürdiger Produkte möglich, ganz egal um welchen charakteristischen Beschaffungsvorgang es sich handelt.

Allgemein ist eine Unterscheidung zwischen strategischen und operativen Beschaffungsprozessen in einer heterogenen Risikolandschaft möglich, um unter Anwendung von wiederholbaren Entscheidungsprozessen vergleichbare Resultate und zuverlässige Beschaffungsergebnisse zu erreichen.

- **Strategische Beschaffungsprozesse:** Dabei handelt es sich um Prozesse, Tätigkeiten und Aufgaben von der ersten Planung und Initiierung bis inklusive dem Abschluss der Auftragserteilung.
- **Operative Beschaffungsprozesse:** Dabei handelt es sich um Prozesse, Tätigkeiten und Aufgaben bis zur Begleichung der Rechnung und umfasst die Entwicklung, den Test und die Abnahme sowie die Inbetriebnahme von Produkten.

A.6.1 Allgemein

A.6.1.1 Beschaffungsarten

Insbesondere die Ausgestaltung eines zyklischen Beschaffungsprozesses hängt auch von der Art einer Beschaffung ab, da gegebenenfalls neben verschiedenen internen Abteilungen auch externe Akteure oder externe Organisationen in die Beschaffungsaktivitäten eingebunden sind:

- **Interne Beschaffung:** Die Beschaffung wird innerhalb der eigenen Organisation durchgeführt.

- **Externe Beschaffung:** Die Beschaffung wird von einer dritten Organisation oder für eine dritte Organisation durchgeführt; oder beides.

A.6.1.2 Beschaffungsvorgänge und Vergabeverfahren

Die generellen Anforderungen im Bereich der IT-Sicherheit sind unabhängig davon ob es sich um eine Ausschreibung oder um eine Direktvergabe bzw. -beschaffung handelt. Charakteristische Vergabeverfahren und damit verbundene Beschaffungsvorgänge haben eine Vielzahl von möglichen Eigenschaften. Generell ist aber eine Unterteilung einerseits in öffentliche oder nicht-öffentliche Verfahren und andererseits in Ausschreibungen, Direktvergaben oder Verhandlungsverfahren möglich.

Zur präziseren Orientierung sind weitere Details über Verfahrensarten zu Vergabeverfahren bzw. indirekt daher auch zu Beschaffungsvorgängen im Bundesvergabegesetz 2018 aufzufinden.

A.6.1.3 Organisationen, Rollen und Akteure im Beschaffungsprozess

- Auftraggeber (z.B.: System-Eigentümer als Organisation, Käuferinnen und Käufer)
- Auftragnehmer (z.B.: Generalunternehmer)
- Zulieferbetriebe (z.B.: Systemlieferanten als Organisation, Teillieferanten, Komponentenlieferanten, Hersteller der Endprodukte, Subauftragnehmer, aber auch Generalunternehmer)
- System-Integrator (z.B.: internes Personal der Auftraggeber oder externe Dienstleister als Organisation)
- System-Operator (operativer bzw. technischer Betrieb wie beispielsweise ein Rechenzentrum)
- Strategische Verantwortungsträger und Entscheider (z.B.: Linienvorgesetzte, Projektmanager)
- Beschaffungsteam (z.B.: Organisatoren, Beschaffer, Sachbearbeiter, Projektteam)
- Anwender (z.B.: Endbenutzer, Endkunden, firmeninterne Kunden)

Darüber hinaus sind weitere Rollen wie etwa externe Berater denkbar um die Phasen einer Beschaffung erfolgreich abzuschließen. Zudem kann eine Beschaffung auch für Dritte (z.B.: im Auftrag für weitere Organisation(en)) durchgeführt werden.

Vor dem Hintergrund, dass eine Vielzahl von Rollen und Organisationen bzw. Abteilungen innerhalb einer Organisation an Beschaffungsprozessen beteiligt sind, ist eine Auflistung und Bereitstellung von Kontaktstellen bzw. umfangreichen Kontaktdetails (z.B.: elektronische Postfächer, persönliche Kontaktdaten) hilfreich für die beteiligten Teams.

A.6.2 Planung einer Beschaffung

A.6.2.1 Phasen für eine sichere Beschaffung

Zur Orientierung für einen möglichen Beschaffungsprozess und damit verbundene Aktivitäten sind hier 10 Phasen für eine sichere Beschaffung beschrieben:

1. Planen und initiieren der Beschaffung (Dieser Schritt kann auch nachdem der Bedarf ermittelt wurde angeordnet sein; Üblicherweise besitzen viele Organisationen einen standardisierten Beschaffungsprozess, der jedoch oft Lücken im Bereich von IT-Sicherheitsaspekten aufweist)
2. Ermitteln des Bedarfs
3. Durchführen einer Marktforschung
4. Ableiten von Produkt-Anforderungen – Entwicklung und Kommunikation
5. Treffen einer Make-or-Buy-Entscheidung (d.h. Eigenanfertigung oder Fremd-Entwicklung)
6. Abwickeln vertraglicher Aspekte (z.B.: Betrieb, Change-Management, Lizenzierung, Wartung)
7. Lieferantenmanagement und Monitoring
8. Abnehmen des Produkts und Akzeptanz (z.B.: finales Testen, Abnahmebericht erstellen)
9. Abschließen des Beschaffungsprojekts
10. Evaluieren des gesamten Prozesses und Produkts im Zusammenhang mit einem Einkaufscontrolling

Die beschriebenen 10 Phasen ermöglichen eine risikobasierte Vorbereitung, Durchführung sowie Evaluation eines Beschaffungsprozesses.

A.6.2.2 Beurteilungskriterien

Wenn die Rahmenbedingungen schon im Vorfeld geklärt, Einflussfaktoren und Randbedingungen festgestellt und relevante Kriterien erarbeitet werden, kann eine fundierte Beurteilung einfacher durchgeführt werden. Daher sollten folgende Kriterien schon zu Beginn definiert werden:

- Kosten im Lebenszyklus des Produkts (Entwicklung, Anschaffung, Änderungen, Betrieb, Wartung; Fixkosten und variable Kosten)

- Anforderungserfüllung (funktionale Anforderungen, nicht-funktionale bzw. Qualitätsanforderungen wie beispielsweise Sicherheit oder Performance)
- Stakeholder-Struktur (Mitwirkung von Dritten, internes Personal, externes Personal, Generalunternehmer, Sub-Auftragnehmer, interne Abteilungen)
- Zeitplanung und Termintreue für die Planung, Design, Konzeption, Umsetzung und die Außerbetriebnahme
- Know-How und Erfahrungen (z.B.: erfolgreich abgeschlossene Projekte) der Stakeholder (intern, extern, abteilungsübergreifend)
- Personal-Struktur (Sicherheitsüberprüfungen, intern oder extern)
- Angewendete Sicherheitsmethoden (z.B.: Vorgehensmodelle, Frameworks, Prozesse) bzw. zugrundeliegende Technologie (z.B.: automatisierte Deployments)

Nachdem im Vorfeld balancierte (z.B.: nach Prioritäten sortierte) Beurteilungskriterien abgeleitet wurden, ist es im Anschluss einfacher eine risikobasierte Beschaffung durchzuführen.

Sonderfall Cloud-Dienste mit künstlicher Intelligenz

Die Beschaffung von KI-Diensten in Cloud-Umgebungen stellt einen etwas spezielleren Beschaffungsvorgang dar, da solche Dienste noch vergleichsweise jung sind und daher auch entsprechend weniger Erfahrungswerte existieren, wodurch eventuell unerkannte Nebeneffekte bzw. unbehandelte Risiken bestehen können auf die im Zuge der Beschaffung nicht eingegangen wird.
Es wird daher empfohlen zusätzlich zu herkömmlichen Beschaffungskriterien noch weitere, auf KI-Dienste fokussierte Kriterien zu betrachten, um auf deren speziellen Eigenschaften einzugehen. Solche Kriterien können zum Beispiel die Zuverlässigkeit, die Datenqualität der für den Dienst benötigten Wissensbasis sowie datenschutzrechtliche Aspekte der Erhebung und Verarbeitung von Daten betreffen.

Hierzu sei auf den Kriterien-Katalog AIC4 (Artificial Intelligence Cloud Service Compliance Criteria Catalogue) des deutschen BSI verwiesen. Dieser spezifiziert Mindestanforderungen für die sichere Verwendung von Anwendungen mit künstlicher Intelligenz, die in Cloud-Diensten betrieben werden. Im Zuge der Beschaffungsvorbereitung solcher KI-Dienste sollten diese Anforderungen mitberücksichtigt werden und somit in die endgültige Beschaffungsentscheidung einfließen.

A.6.2.3 Basis-Sicherheitsanforderungen nach ENISA

Gerade wenn Produkte wie beispielsweise Software, oder integrierte Hardware-Software-Kombinationen (Embedded-Systeme) extern zugekauft werden, sind auch oft Sub-Auftragnehmer an der Konzeption, der Spezifikation, dem Design, der Entwicklung, dem Test und oft auch während der Inbetriebnahme oder im Produktionsbetrieb beteiligt.

Daher ist es für komplexe Lieferantenbeziehungen von Bedeutung, dass sowohl der Lieferant, als auch seine Zulieferer und Service-Provider IT-Sicherheitsaspekte berücksichtigen und notwendige Minimalanforderungen im Bereich der IT-Security erfüllen. Nach ENISA [ENISA12-2016] handelt es sich dabei um:

- **Security by design** (Eingestelltes und konfiguriertes Produkt bei Auslieferung auf der Grundlage von etablierte Sicherheitspraktiken)
- **Least privilege** (Administrative Rechte werden nur wann, wie und wo absolut unerlässlich verwendet. Das Produkt wird normalerweise mit eingeschränkten Rechten genützt.)
- **Strong authentication** (z.B.: zuverlässige Zweifaktor oder Mehrfaktorauthentifizierung mittels Token/Smartcard/App. Wenn Authentifizierung nicht erfolgreich ist, dann sind benutzerzentrierte Aktivitäten nicht möglich)
- **Asset protection** (Schutz kritischer Daten, Prozesse und von Know-How)
- **Supply chain security** (Wahrung der Integrität eines Produkts während des Lebenszyklus)
- **Transparente Dokumentation** (Erstellen verständlicher und umfangreicher – sinnvoller – Dokumentationen über das entwickelte Produkt)
- **Qualitätsmanagement** (Prozessorientierte Vorgehensweise nach sicheren Software-Entwicklungsprinzipien, Qualitätsmanagement und Informationssicherheitsmanagement als Fundament im Bereich der IT-Security)
- **Service-Kontinuität** (Service-Level-Agreements um Support während des Lebenszyklus eines Produkts zu gewährleisten)
- **EU-Rechtslage** (Entwickeln des Produkts unter Akzeptanz der EU-Rechtsnormen und der nationalen Rechtsvorschriften)
- **Einschränkung der Datennutzung** (Deklarieren welche Daten wie verarbeitet, übertragen oder gespeichert werden)

Weiters empfiehlt ENISA relevante IKT-Standards bestmöglich zu nützen um kosteneffektive Akquisitionen von IKT-Produkten durchzuführen. Ein möglicher internationaler Standard für eine Umsetzung eines praktisch nutzbaren Akquisitionsprozesses ist ISO/IEC 12207.

A.6.2.4 Begleitende Risikoanalyse

Beschaffung von Komponenten aus externen Quellen ist ein Risikofaktor im Lebenszyklus von Produkten. Daher ist eine vernünftige Ableitung des Schutzbedarfs auf der Grundlage durchgeführter Risikoanalysen zweckmäßig. In manchen Fällen kann ein sogenanntes vorvertragliches Vertrauensverhältnis die Risiken reduzieren.

Bereits vor der Initiierung einer Beschaffung sowie während des Beschaffungsvorgangs und darüber hinaus auch nach der Vertragsbeendigung (z.B.: zur Außerbetriebnahme des angeschafften Produkts) sind insbesondere die kontinuierliche Risiko-Identifizierung, Risiko-Bewertung, Risiko-Dokumentation und die Ableitung von Risikoreduktionsmaßnahmen (auch Risikokontrollmaßnahmen) erfolgskritisch. Weitere Details zur Risikoanalyse sind in Abschnitt 5.1 beschrieben. Dies umfasst auch eine Bedrohungsanalyse und eine Schwachstellenanalyse der betroffenen Systeme.

A.6.2.5 Produktarten

Übersicht der gängigen Arten von Produkten die beschafft werden können:

- **Commercial off-the-shelf, COTS**
  Bereits vorhandene Standard-Produkte (z.B.: Software) die in größeren Stückzahlen von kommerziellen Anbietern – außerhalb der beschaffenden Organisation – bereitgestellt werden. Die Beschaffung ereignet sich im Rahmen des üblichen Geschäftsprozesses auf der Grundlage von Marktpreisen oder Katalogen. Diese Produkte werden in eine bestehende technische Infrastruktur integriert. COTS wird dabei auch als Überbegriff für Produkte verwendet, die von externen Quellen zugekauft werden. Überwiegend handelt es sich um „Closed-Source“-Produkte.
- **Government off-the-shelf, GOTS**
  Von Regierungsorganisationen oder von Ministerien entwickelten Produkte welche im Eigentum dieser Organisationen stehen und in diesem Umfeld genützt werden. Die Entwicklung erfolgt üblicherweise für eine maßgeschneiderte Problemlösung dedizierter Probleme im Bereich der öffentlichen Verwaltung. Eingesetzt wird dabei entweder internes oder technisches Personal der Regierungsorganisation. Die Beschaffung ereignet sich beispielsweise über regierungseigene Beschaffungsplattformen. Oft handelt es sich hier um Produkte, deren Source-Code geheim gehalten oder patentiert wird bzw. nicht-öffentlich abrufbar ist. In manchen Fällen jedoch ist das zugrundeliegende Know-How teilweise oder vollständig öffentlich zugänglich.
- **Individuelle Neuentwicklung**
  Auf der Grundlage von identifizierten Anforderungen und meistens wegen einzigartigen Bedürfnissen (z.B.: besondere Datenschutzanforderungen) werden beispielsweise Software-Produkte maßgeschneidert für eine konkrete Problemlösung auf der grünen Wiese entwickelt. Die dabei erstellten, oft subjektiven, Bedarfsermittlungen liefern die erste Grundlage für eine solche Neuentwicklung.
- **Individuelle Anpassung bestehender Produkte**

Wenn bereits bestehende Produkte geringfügig oder umfangreich für die Anforderungen (z.B.: Funktionsumfang, Qualitätsanforderungen) angepasst werden, dann handelt es sich um individuelle Änderungen bestehender Produkte.

- **Open-Source-Produkte**
  Open-Source-Produkte bzw. das zugrundeliegende Know-How (z.B.: Source-Code) sind öffentlich zugänglich. Bezeichnet wird dies auch als „quell-offene Software“.

Je nach Art des zu beschaffenden Produkts – und insbesondere der Ausprägung bzw. der Umfang der zu erfüllenden Anforderungen – bestehen unterschiedliche Risiken, die bereits im Vorfeld in durchzuführende Risiko-Analysen einfließen sollten, um bereits frühzeitig IT-Sicherheitsaspekte in den Beschaffungsprozess zu integrieren.

A.6.2.6 IT-Sicherheitsrisiken der einzelnen Produktarten

Jede Situation ist individuell und Beschaffungsrisiken sind organisationsspezifisch. Im Folgenden sind einige Beispiele für potenzielle IT-Sicherheitsrisiken der jeweiligen Produktarten aufgelistet:

COTS

- Bindung an einen Zulieferer (z.B.: Single-Vendor-Lock-In) bzw. eine konkrete (z.B.: unflexible) Technologie und fehlende Redundanz
- Bindung des Expertenwissens außerhalb der beschaffenden Organisation
- Geschlossenes System als Blackbox wodurch das Innenleben für Kunden nicht einsehbar ist
- Überflüssige Funktionen, die nicht den Anforderungen entsprechen, als Sicherheitsrisiko
- Qualitätsanforderungen können architekturbedingt nur teilweise eingehalten werden
- IT-Sicherheit wurde erst im Nachhinein berücksichtigt und „hinzugefügt“ statt auf dem Prinzip „Security-by-Design“ zu basieren
- Komplexe Integration in die bestehende technische Infrastruktur der Kunden
- Fehleranfällige Deployments
- Aufwändiges Change-Management
- Unzureichende Einsicht in die Entwicklungsprozesse und die installierten Sicherheitsmaßnahmen beim Zulieferer
- Eine Vertrauensbeziehung ist im Vorfeld oft notwendig (z.B.: Personal-Risiken)
- Hoher Abstimmungsaufwand bei externen Beschaffungen
- Anpassung betrieblicher Prozesse an die Software kann notwendig sein

GOTS

- Standardisierte Beschaffungsprozesse (z.B.: individuelle Bedürfnisse im Bereich der IT-Sicherheit können nicht oder nicht ausreichend abgedeckt werden)
- Sehr spezifische Problemlösungen, die oft hohe Adaptierungsmaßnahmen erfordern
- Beteiligung einer Vielzahl von Stakeholdern
- Wiederverwendbarkeit ist überwiegend auf den öffentlichen Bereich eingeschränkt
- Hoher Abstimmungsaufwand bei externen Beschaffungen

Individuelle Neuentwicklung

- Fehlendes Know-How innerhalb der Organisation
- Bestehende Problemlösungen in der Regel unzureichend berücksichtigt
- Hoher Zeitaufwand für Entwicklung und Betrieb
- Sehr hoher Spezialisierungsgrad und hohe Erfordernisse an spezifisches Know-How

Individuelle Anpassung bestehender Produkte

- Aufwändige Adaptierungen um die Anforderungen zu erfüllen
- Überflüssige Funktionen, die nicht den Anforderungen entsprechen als Risiko
- Unzureichende Schnittstellen die nicht die Anforderungen der Nutzerinnen und Nutzer erfüllen (z.B.: User-Interface, Verknüpfung mit anderen Modulen)
- Die Adaptierung ist sehr kostenintensiv und kann selten innerhalb der beschaffenden Organisation durchgeführt werden
- Manche Anpassungen sind architekturbedingt nicht möglich (z.B.: technologieabhängige Schwachstellen)

Open-Source-Produkte

- Ausnützen von Schwachstellen da z.B.: der Source-Code öffentlich zugänglich ist
- Verbreitung von geschütztem Know-How (z.B.: Adaptierungen)
- Lizenzierung ist kompliziert (z.B.: Resultate, die mit Open-Source-Produkten erstellt werden, müssen manchmal auch öffentlich zugänglich sein)
- Technischer Support nicht vorhanden oder ist ressourcenintensiv
- Zuverlässigkeit der Weiterentwicklung manchmal nicht vorhersehbar

A.6.3 Auswahl und Umsetzung einer Beschaffung

A.6.3.1 Akquisitionsprozess nach ISO/IEC 12207

Die Beschaffung von Produkten ist in den Lebenszyklus des Produkts integriert. Im Gegensatz zu einer Eigenanfertigung bzw. einer eigenen Inhouse-Entwicklung ist die Fremdentwicklung und die damit verbundene Beschaffung im Rahmen einer Make-or-Buy-Entscheidung zu definieren. Ist die Entscheidung für eine Akquisition (Buy-Entscheidung) gefallen ist beispielsweise das folgende Prozessmodell mit 5 Prozessschritten – nach ISO/IEC 12207 – anwendbar:

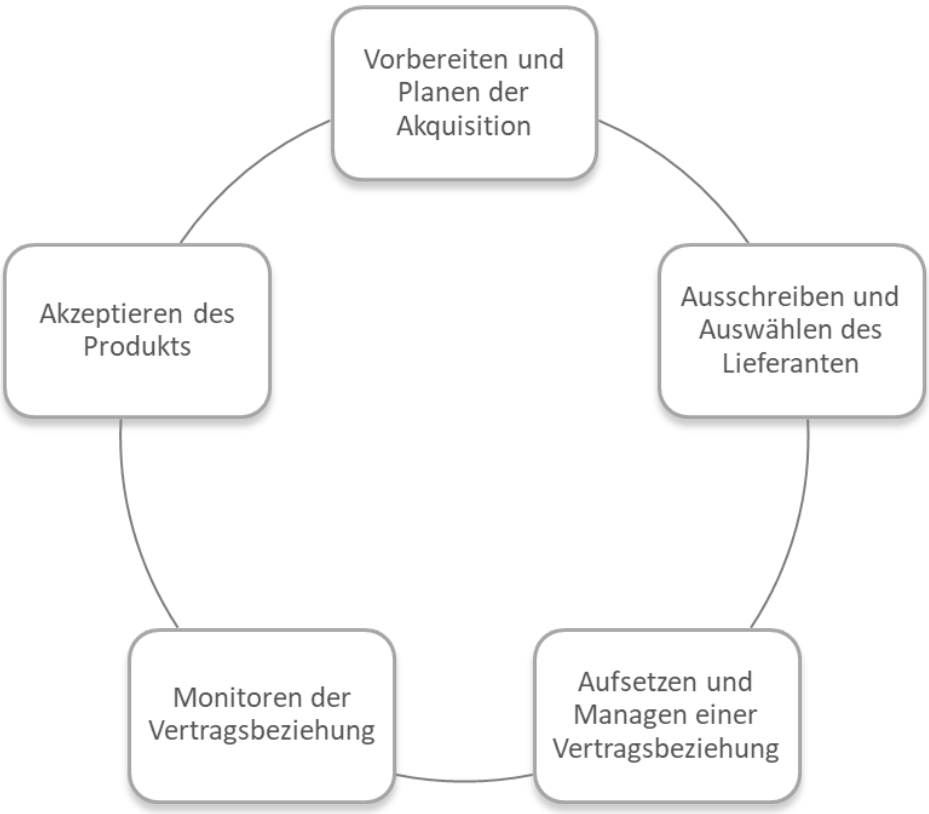

Abbildung A.6.1: Akquisitionsprozess nach ISO/IEC 12207

A.6.3.2 Vorbereiten und Planen der Akquisition

Diese strategische Aufgabe umfasst Tätigkeiten um die Planung sowie die Herangehensweise an die bevorstehende Beschaffung vorzubereiten und wie diese durchzuführen ist. Darin sind enthalten:

- Lebenszyklusmodell des Produkts festlegen
- Risiken, Bedrohungen und potenzielle Schwachstellen untersuchen, evaluieren und dokumentieren
- Schutzbedarf aus erkannten Risiken ableiten

- Projektplanung und zeitlichen Ablauf definieren
- Pflichten und Verantwortungen sowie damit verbundene, relevante Rollen herausarbeiten
- Auswahlkriterien für Lieferanten erarbeiten und klassifizieren
- Anzuwendende Methoden und Modelle eingrenzen
- Prioritäten einordnen und sortieren
- Erstellen eines Anforderungskatalogs für ein Produkt oder ein Service

A.6.3.3 Ausschreiben und Auswählen des Lieferanten

Dieser strategische Prozessschritt umfasst zumindest die folgenden Aktivitäten:

- Aussenden (z.B.: veröffentlichen, oder nicht-öffentlich Bereitstellen) der Anforderungsdokumente an potenzielle Zulieferer
- Auswählen eines oder mehrerer Zulieferer auf der Grundlage evaluierter und verglichener Auswahlkriterien

A.6.3.4 Aufsetzen und Managen einer Vertragsbeziehung

Dieser strategische Beschaffungsschritt beinhaltet die Aufgaben und Tätigkeiten, um mit dem Zulieferer bzw. dem Lieferanten einen abgestimmten und rechtlich adäquaten Vertrag abzuschließen und in weiterer Folge die vereinbarten Leistungen (z.B.: Software-Produkt entwickeln) bzw. Gegenleistungen (z.B.: Entgelt bezahlen) zu erfüllen.

- Entwickeln eines Vertrags mit dem Lieferanten welcher die abgeleiteten Akzeptanzkriterien enthält
- Identifizieren, prüfen und evaluieren sowie integrieren notwendiger Änderungen für den bzw. in den Vertrag
- Verhandeln und abschließen der Vertragsbeziehung

Am Ende besteht ein ausgehandelter und zu erfüllender Vertrag zwischen Auftraggeber und Auftragnehmer.

IT-Sicherheitsanforderungen

Um IT-Sicherheitsanforderungen auszuarbeiten, ist die Auseinandersetzung mit den funktionalen und qualitativen Anforderungen sowie den damit verbundenen IT-Security-Aspekten erforderlich. Aus dem erkannten Schutzbedarf und der damit verknüpften Kritikalität des zu beschaffenden Systems bzw. Produkts ist die Ableitung von IT-Sicherheitsanforderungen möglich. Die wesentliche Berücksichtigung von Anforderungen aus der IT-Sicherheit gegenüber dem Auftragnehmer kann beispielsweise durch die Forderung zur Vorlage von

Evidenz-Unterlagen (z.B.: Eignungsnachweise, Zeugnisse, Zertifikate) verlangt werden um etwa Sicherheitsupdates systematisch einzupflegen. Auch ist die Forderung nach dem Einsatz von zertifizierten Produkten, Dienstleistungen oder auch nach Personenzertifikaten denkbar. Darüber hinaus sind in der erstellten Anforderungsdokumentation auch IT-Sicherheitskriterien zu verankern.

Sicherheitsupdates und Change-Management

Vor dem Hintergrund der Berücksichtigung von IT-Security-Aspekten muss der beauftragte Zulieferer Sicherheitsupdates für alle integrierten Systemkomponenten während des vollständigen, vertraglich definierten Entwicklungs- und Betriebszeitraums bereitstellen. Darüber hinaus muss der beauftragte Zulieferer System-Aktualisierungen (z.B.: Updates, Security-Patches) von Systemen, die nicht vom Zulieferer entwickelt wurden, vom jeweiligen Hersteller beschaffen, testen und je nach vorliegender Vertragsausgestaltung integrieren bzw. an den Auftraggeber in geeigneter Form übermitteln. Die Bereitstellung der notwendigen Aktualisierungen muss innerhalb eines vertraglich definierten, jedoch angemessenen Zeitrahmens abgeschlossen sein. Der Auftragnehmer muss einen dokumentierten Prozess installiert haben, um Sicherheitslu#cken zu beheben.

Zertifizierungen von Produkten, Systemen, Personen und Organisationen

Zertifizierungen bestätigen, dass zu einem bestimmten Zeitpunkt, eine definierte Menge an Anforderungen eingehalten wurden und die Prüfung nach einem festgelegten Verfahren durchgeführt wurde.

Produkt-Zertifizierungen: International anerkannte und weit verbreitet angewendete Zertifizierungsverfahren für z.B.: kryptographische Produkte stellen im Bereich der IT-Sicherheit einen wesentlichen Baustein für die Zuverlässigkeit der geprüften Produkte und die nachvollziehbar angewendeten Methoden dar. Beispiele für Produktzertifizierungen aus dem IT-Security-Bereich sind:

- ISO/IEC 15408 (Information technology – Security techniques; auch: Common Criteria)
- NIST FIPS 140-2 (Federal Information Processing Standard (FIPS) Publication 140-2)

System-Zertifizierungen: Systeme zum Management von Informationssicherheitsaspekten ermöglichen die Sicherstellung eines geordneten Umgangs mit Informationssicherheit in einer Organisation. Beispiele für System-Zertifizierungen aus dem Informationssicherheitsumfeld bzw. mit Relevanz für IT-Sicherheitsaspekte sind:

- ISO/IEC 27001 (Information technology – Security techniques)
- ITIL (Information Technology Infrastructure Library; z.B.: ITIL Security Management)

Personen-Zertifizierungen: Wenn die Kritikalität eines zu beschaffenden Systems bei einer Individualentwicklung hoch ist, dann ist es mitunter sinnvoll, vom Auftragnehmer zu fordern, dass das eingesetzte Personal bestimmte Personen-Zertifizierungen hält. Davon gibt es eine ganze Reihe kommerzieller Organisationen, die derartige Personen-Zertifizierungen anbieten.

Organisationszertifzierungen: Gerade im Bereich der IT-Sicherheit ist auch Qualität ein hervorzuhebender Faktor, der Auswirkungen auf das erreichbare Sicherheitsniveau von Produkten hat. Beispiele für Zertifizierungen von Organisationen mit Bezug zur IT-Sicherheit sind:

- ISO 9001 (Qualitätsmanagementsysteme)

A.6.3.5 Monitoren der Vertragsbeziehung

Als operativer Teilprozess der Beschaffung ist eine laufende Überprüfung der Ausübung der vertraglich festgelegten Pflichten aber auch der damit verbundenen Rechte erforderlich. Damit ist die zeitgerechte Lösung auftretender Probleme (z.B.: fehlende Daten) möglich. Darin enthalten sind:

- Regelmäßige Bestätigungen erstellen, dass die Pflichten erfüllt werden (Auftraggeber – z.B.: Zahlung und Auftragnehmer – z.B.: Teilsysteme liefern)
- Evaluieren des Projekt-Fortschritts (z.B.: Projektplanung, Meilensteine, Arbeitspakete, Kosten)
- Akzeptanztests zur Abnahme des Produkts

A.6.3.6 Akzeptanz des Produkts

Nachdem das Produkt so weit entwickelt ist, um an den Auftraggeber ausgeliefert zu werden, ist vor dem Hintergrund von IT-Sicherheitsanforderungen die Abnahme des entstandenen Produkts erforderlich.

Die Abnahme umfasst eine Prüfung ob das entstandene Produkt quantitativ messbare bzw. qualitativ relevante Anforderungen oder funktionale Anforderungen erfüllt. Darüber hinaus setzt eine erfolgreiche Abnahme voraus, dass die notwendigen – spezifizierten Anforderungen im Produktivsystem korrekt integriert sowie verfügbar sind. Vor dem Hintergrund der IT-Sicherheit sind nicht erforderliche Eigenschaften oder Funktionen von Computer-Systemen zu hinterfragen und insbesondere im Hinblick auf mögliche Schwachstellen und damit verknüpfte Risiken zu evaluieren. Die folgenden Anforderungen können in Verträge, Service-Level-Agreements, Standards bzw. betriebliche Vereinbarungen integriert werden:

- Gewährleisten des aktuellen Stands der Technik

- Definieren von Schlüsselzielen (z.B.: Key Goal Indicators, Key Performance Indicators, Key Risk Indicators)
- Integration von Best-Practices (z.B.: Plan-Do-Check-Act-Zyklus)
- Überprüfen, auditieren und reviewen von Informationssicherheitsaspekten (z.B.: Strategien, Frameworks, Policies, Richtlinien, Zertifizierungen)
- Verifizieren der Integrität von Computersystemen im laufenden Betrieb
- Bereitstellen und überprüfen des vollständigen Source-Codes (z.B.: Audit, Source-Code-Review, Architektur-Reviews)
- Vertragliche Verpflichtung zur Einhaltung strikter Regeln und Verfahren (z.B.: Freiheit von Schadsoftware, Verpflichtung zur Behebung von Schwachstellen)
- Zeitlich angemessenes reagieren um Schwachstellen zu beheben
- Installieren von Sicherheitssystemen (z.B.: Intrusion Detection Systeme, Intrusion Prevention Systeme, Security Information and Event Management, Malware Defense)
- Durchführen von Tests (z.B.: Qualifikationstests, Penetration-Tests, Sicherheitstests, Schwachstellenanalysen)
- Sicherheitsnormen, Best-Practices und Richtlinien einhalten
- Staging-Konzept zur Durchführung von Qualifikationstests beim Zulieferer etablieren
- Wartungskonzept für das Produktionssystem installieren
- Inbetriebnahme-Unterstützung durch den Zulieferer festlegen (gilt auch für etwaige Außerbetriebnahme in der Zukunft)
- Plan zur Inbetriebnahme (und zur späteren Außerbetriebnahme) erarbeiten
- Einschulung und Training für das Betriebspersonal und die Endnutzer
- Vereinbarungen zur Gewährleistung und Garantie etablieren

Je nach Anwendungsbereich und Kritikalität des zu beschaffenden Produkts, kann diese Liste entweder erweitert oder verkürzt werden. Zu diesem Zweck stellt die Beschaffungsplattform IT-SICHER.kaufen – mit dem Fokus des Einkaufs von Software-Produkten – relevante Inhalte für Beschaffungen (sogenannte Beschaffungstexte) zur Verfügung. Damit können konkrete IT-Sicherheitsanforderungen ausgewählt werden und Checklisten erstellt werden. Zudem liefert diese österreichische Plattform abrufbare Auflistungen von Produkten und die Herkunft der Hersteller um etwa die bereits erwähnte Vertrauenskomponente abzudecken. Darüber hinaus werden Schutzbedarfsklassifizierungen sowie konkrete Empfehlungen für anwendbare kryptographische Algorithmen und zuverlässige Schlüssellängen bzw. Passwortrichtlinien behandelt.

B Muster für Verträge, Verpflichtungserklärungen und Dokumentationen

Im Folgenden sind Musterverträge, Verpflichtungserklärungen etc. als PDF-Dateien abrufbar. Zum Öffnen bzw. zum Betrachten der Dateien kann der Acrobat Reader (frei erhältlich unter https://www.adobe.com/at/) oder ein sonstiges PDF-Tool verwendet werden.

B.1 Sourcecodehinterlegung (Muster, aus AVB-IT)

B.2 *(obsolet)*

B.3 Fehlerklassen Wartung (Muster, aus AVB-IT)

B.4 Verpflichtungserklärung betreffend die Benutzung von IT-Systemen (Muster)

B.5 *(obsolet)* - Mustervorlagen zu Standardvertragsklauseln für die Auftragsverarbeitung nach EU-DSGVO finden Sie auf der Webseite der Österreichischen Datenschutzbehörde. Ein Mustervertrag für die Auftragsverarbeitung ist auf der Webseite der Wirtschaftskammer Österreich verfügbar.

B.6 Verpflichtungserklärung zur Einhaltung des DSG für öffentlich Bedienstete (Muster)

B.7 Verpflichtungserklärung zur Einhaltung des DSG für Dienstnehmer eines (privaten) Auftragsverarbeiters (Muster)

B.8 Verpflichtungserklärung zur Nutzung von dienstlich bereitgestellten mobilen Geräten (Notebooks) (Muster)

B.9 *(obsolet)*

B.10 Inhaltsverzeichnis Virenschutzkonzept (Muster)

B.11 Inhaltsverzeichnis Kryptokonzept (Muster)

B.12 Inhaltsverzeichnis Datensicherungskonzept (Muster)

B.13 Inhaltsverzeichnis Disaster Recovery-Handbuch (Muster) (alternativ auch als Notfallhandbuch bezeichnet)

C.1 Wichtige Normen

Im Folgenden wird eine Reihe von Normen, die für die einzelnen Themenbereiche von Interesse sein können, angeführt. Aufgrund der Vielzahl von nationalen und internationalen Normen können im Rahmen dieses Handbuchs keinesfalls alle Dokumente angegeben werden. Es empfiehlt sich daher bei eingehender Beschäftigung mit einem Themenbereich, weitere Recherchen, entweder ausgehend von den angeführten Normen oder über entsprechende Datenbanken oder Institutionen (z. B. ÖNORM), durchzuführen. Hier sei auch besonders auf die in F Wichtige Adressen angegebenen Internetadressen verwiesen.

Normen sind einer laufenden Überprüfung und Weiterentwicklung unterworfen. Daher wurde in den nachfolgenden Zusammenstellungen auf eine Angabe von Status (z. B. Norm, Vornorm, …) und Ausgabedatum verzichtet.

Brandschutz

ÖNORMEN:

B 3800	Brandverhalten von Baustoffen und Bauteilen
B 3850	Feuerschutzabschlüsse - Drehflügeltüren und -tore sowie Pendeltüren - Ein- und zweiflügelige Ausführung
B 3858	Türschlösser - Einsteckschlösser für Feuerschutzabschlüsse - Anforderungen und Prüfungen
EN 2	Brandklassen
EN 3	Tragbare Feuerlöscher
EN 54	Brandmeldeanlagen
EN 13501	Klassifizierung von Bauprodukten und Bauarten zu ihrem Brandverhalten
EN ISO 7010	Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Registrierte Sicherheitszeichen
F 2030	Kennzeichnung für den Brandschutz - Anforderungen, Ausführung, Verwendung und Anbringung
F 2031	Planzeichen für Brandschutzpläne

TRVB Technische Richtlinie Vorbeugender Brandschutz
Die TRVB werden vom Österreichischen Bundesfeuerwehrverband und den Brandverhütungsstellen der Länder herausgegeben.

Der Gruppenbuchstabe in der TRVB-Nummer bedeutet:

A	=	Allgemein
B	=	Bauwesen

C	=	Chemie
E	=	Elektrotechnik
F	=	Abwehrender Brandschutz
H	=	Heizungsanlagen, Feuerstätten
L	=	Landwirtschaft
N	=	Nutzung von Gebäuden und Gebäudeteilen
O	=	Organisation
S	=	Selbsttätige Brandschutzeinrichtungen

Auswahl aus den TRVB:

A 100/10	Brandschutzeinrichtungen - Rechnerischer Nachweis
A 101/67	Grundlagen für die Beurteilung der Brand- und Explosionsgefährlichkeit
E 102/05	Fluchtweg - Orientierungsbeleuchtung
O 119/06	Betriebsbrandschutz - Organisation
O 120/06	Betriebsbrandschutz - Eigenkontrolle - Kontrollplan
O 121/15	Brandschutzpläne für den Feuerwehreinsatz
S 122/13	Rauchwarnmelder
S 123/11	Brandmeldeanlagen
F 124/97	Erste und Erweiterte Löschhilfe
S 125/15	Rauch- und Wärmeabzugsanlagen und Rauchableitungsanlagen
A 126/87	Brandschutztechnische Kennzahlen verschiedener Nutzungen, Lagerungen, Lagergüter
S 127/11	Sprinkleranlagen
S 128/12	Ortsfeste Löschanlagen nass und trocken
F 134/87	Aufstellungsflächen für die Feuerwehr auf Grundstücken
B 148/84	Feststellanlagen für Brand- und Rauchabschlüsse
S 151/15	Brandfallsteuerungen
S 152/15	Gaslöschanlagen

Sicherheitstüren und einbruchhemmende Türen

ÖNORMEN:

B 3850	Feuerschutzabschlüsse - Drehflügeltüren und -tore sowie Pendeltüren - Anforderungen und Prüfungen für ein- und zweiflügelige Elemente

B 3858	Türschlösser - Einsteckschlösser für Feuerschutzabschlüsse - Anforderungen und Prüfungen
B 5338	Einbruchhemmende Fenster, Türen und zusätzliche Abschlüsse - Allgemeine Festlegungen
B 5351	Einbruchhemmende Baubeschläge - Schlösser, Schließbleche, Schutzbeschläge, Schließzylinder und Nachrüstprodukte für Fenster und Türen - Maße, Ausführung, Prüfung und Kennzeichnung

Wertbehältnisse

ÖNORMEN:

EN	1047-1	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsschränke und Disketteneinsätze
EN	1047-2	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Datensicherungsräume und Datensicherungscontainer
EN	1143	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl
EN	1300	Wertbehältnisse - Klassifizierung von Hochsicherheitsschlössern nach ihrem Widerstandswert gegen unbefugtes Öffnen
EN	14450	Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl - Sicherheitsschränke
EN	15659	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Leichte Brandschutzschränke

Vernichtung von Akten und Daten

ÖNORMEN:

S 2109	Akten- und Datenvernichtung

Informationssicherheit und IT-Sicherheit

ISO und IEC-NORMEN:

ISO/IEC 2382:2015	Information technology - Vocabulary
ISO/IEC 7064:2003	Information technology - Security techniques - Check character systems
ISO/IEC 7816-4:2013	Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange
ISO 9564-1:2011	Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card-based systems

ISO 9564-2:2014	Financial services - Personal Identification Number (PIN) management and security - Part 2: Approved algorithms for PIN encipherment
ISO/TR 9564-4:2004	Banking - Personal Identification Number (PIN) management and security - Part 4: Guidelines for PIN handling in open networks
ISO/IEC 9579:2000	Information technology - Remote database access for SQL with security enhancement
ISO/IEC 9594-Parts 1-9:2014	Information technology - Open Systems Interconnection - The Directory
ISO/IEC 9796-2:2010	Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2006	Information technology - Security techniques - Digital signature scheme giving message recovery - Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:2011	Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2011	Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9797-3:2011	Information technology - Security techniques - Message Authentication Codes (MACs) - Part 3: Mechanisms using a universal hash-function
ISO/IEC 9798-1:2010	Information technology - Security techniques - Entity authentication - Part 1: General
ISO/IEC 9798-2:2008	Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms
ISO/IEC 9798-3:1998	Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999	Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:2009	Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques
ISO/IEC 9798-6:2010	Information technology - Security techniques - Entity authentication - Part 6: Mechanisms using manual data transfer
ISO/IEC 10116:2006	Information technology - Modes of operation for an n-bit block cipher

ISO/IEC 10118-1:2000	Information technology- Security techniques - Hash functions - Part 1: General
ISO/IEC 10118-2:2010	Information technology- Security techniques - Hash functions - Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-3:2004	Information technology- Security techniques - Hash functions - Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998	Information technology- Security techniques - Hash functions - Part 4: Hash-functions using modular arithmetic
ISO/IEC 10164-7:1992	Information technology - Open Systems Interconnection - Systems Management: Security alarm reporting function
ISO/IEC 10164-8:1993	Information technology - Open Systems Interconnection - Systems Management: Security audit trail function
ISO/IEC 10181-Parts 1-7:1996	Information technology - Open systems interconnection - Security frameworks for open systems
ISO/IEC 10736:1995	Information technology - Telecommunications and information exchange between systems - Transport layer security protocol
ISO/IEC 10745:1995	Information technology - Open Systems Interconnection - Upper layers security model
ISO 11568-2:2012	Banking - Key management (retail) - Part 2: Symmetric ciphers, their key management and life cycle
ISO 11568-4:2007	Banking - Key management (retail) - Part 4: Asymmetric cryptosystems - Key management and life cycle
ISO/IEC 11577:1995	Information technology - Open Systems Interconnection - Network layer security protocol
ISO/IEC 11586-Parts1-6:1996	Information technology - Open Systems Interconnection - Generic upper layers security
ISO/TR 11633-1:2009	Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis
ISO/TR 11633-2:2009	Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)
ISO/IEC 11770-1:2010	Information technology - Security Techniques - Key Management - Part 1: Framework
ISO/IEC 11770-2:2008	Information technology - Security Techniques - Key Management - Part 2: Mechanisms using symmetric techniques

ISO/IEC 11770-3:2015	Information technology - Security Techniques - Key Management - Part 3: Mechanisms using asymmetric techniques
ISO/IEC 11770-4:2006	Information technology - Security Techniques - Key Management - Part 4: Mechanisms based on weak secrets
ISO/IEC 11770-5:2011	Information technology - Security Techniques - Key Management - Part 5: Group key management
ISO/IEC 12207:2017	Systems and software engineering — Software life cycle processes
ISO/IEC 13157-1:2014	Information technology - Telecommunications and information exchange between systems - NFC Security - Part 1: NFC-SEC NFCIP-1 security services and protocol
ISO/IEC 13157-2:2010	Information technology - Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES
ISO 13491-1:2007	Banking - Secure Cryptographic devices (retail) - Part 1: Concepts, requirements and evaluation methods
ISO 13491-2:2005	Banking - Secure Cryptographic devices (retail) - Part 2: Security compliance checklists for devices used in financial transactions
ISO 13492:2007	Financial services - Key management related data element - Application and usage of ISO 8583 data elements 53 and 96
ISO/TR 13569:2005	Financial services - Information security guidelines
ISO/IEC TR 13594:1995	Information technology - Lower layers security
ISO/TS 13606-4:2009	Health informatics - Electronic health record communication - Part 4: Security
ISO/IEC 13888-1:2009	Information technology - Security techniques - Non-repudiation - Part 1: General
ISO/IEC 13888-2:2010	Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques
ISO/IEC 13888-3:2009	Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques
ISO/TS 14441:2013	Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment
ISO/IEC TR 14516:2002	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services

ISO/TR 14742:2010	Financial services - Recommendations on cryptographic algorithms and their use
ISO/IEC 14888-1:2008	Information technology - Security techniques - Digital signatures with appendix - Part 1: General
ISO/IEC 14888-2:2008	Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms
ISO/IEC 14888-3:2006	Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms
ISO/IEC TR 15067-4:2001	Information technology - Home Electronic System (HES) Application Model - Part 4: Security System for HES
ISO/IEC 15149:2016	Information technology - Telecommunications and information exchange between systems - Magnetic field area network (MFAN) - Part 4: Security Protocol for Authentication
ISO/IEC 15408-1:2009	Information technology- Security techniques- Evaluation criteria for IT security - Part 1: Introduction and general model
ISO/IEC 15408-2:2008	Information technology- Security techniques- Evaluation criteria for IT security - Part 2: Security functional components
ISO/IEC 15408-3:2008	Information technology- Security techniques- Evaluation criteria for IT security - Part 3: Security assurance components
ISO/IEC TR 15443-1:2012	Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts
ISO/IEC TR 15443-2:2012	Information technology - Security techniques - Security assurance framework - Part 2: Analysis
ISO/IEC TR 15446:2009	Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets
ISO/IEC 15816:2002	Information technology - Security techniques - Security information objects for access control
ISO/IEC 15945:2002	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:2008	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General
ISO/IEC 15946-5:2009	Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation

ISO/IEC TR 16166:2010	Information technology - Telecommunications and information exchange between systems - Next Generation Corporate Networks (NGCN) - Security of session-based communications
ISO/IEC 16500-7:1999	Information technology - Generic digital audio-visual systems - Part 7: Basic security tools
ISO 17090-1:2013	Health informatics - Public key infrastructure - Part 1: Overview of digital certificate services
ISO 17090-2:2015	Health informatics - Public key infrastructure - Part 2: Certificate profile
ISO 17090-3:2008	Health informatics - Public key infrastructure - Part 3: Policy management of certification authority
ISO 17090-4:2014	Health informatics - Public key infrastructure - Part 4: Digital Signatures for healthcare documents
ISO/TS 17574:2009	Electronic fee collection - Guidelines for security protection profiles
ISO/IEC 17825:2016	Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
ISO/IEC 18014-1:2008	Information technology - Security techniques - Time-stamping services - Part 1: Framework
ISO/IEC 18014-2:2009	Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens
ISO/IEC 18014-3:2009	Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens
ISO/IEC 18014-4:2015	Information technology - Security techniques - Time-stamping services - Part 4: Traceability of time sources
ISO/IEC 18031:2011	Information technology - Security techniques - Random bit generation
ISO/IEC 18032:2005	Information technology - Security techniques - Prime number generation
ISO/IEC 18033-1:2015	Information technology - Security techniques - Encryption algorithms - Part 1: General
ISO/IEC 18033-2:2006	Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers
ISO/IEC 18033-3:2010	Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers
ISO/IEC 18033-4:2011	Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers

ISO/IEC 18033-5:2015	Information technology - Security techniques - Encryption algorithms - Part 5: Identity-based ciphers
ISO/IEC 18045:2008	Information technology - Security techniques - Methodology for IT security evaluation
ISO 19092:2008	Financial services - Biometrics - Security framework
ISO/TS 19299:2015	Electronic fee collection - Security framework
ISO/IEC 19772:2009	Information technology - Security techniques - Authenticated encryption
ISO/IEC 19785-4:2010	Information technology - Common Biometric Exchange Formats Framework - Part 4: Security block format specifications
ISO/IEC 19790:2012	Information technology - Security techniques - Security requirements for cryptographic modules
ISO/IEC TR 19791:2010	Information technology - Security techniques - Security assessment of operational systems
ISO/IEC 19792:2009	Information technology - Security techniques - Security evaluation of biometrics
ISO/IEC TR 20004:2015	Information technology - Security techniques - Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC 20008-Parts 1-2:2013	Information technology - Security techniques - Anonymous digital signatures
ISO/IEC 20009-Parts 1-2:2013	Information technology - Security techniques - Anonymous entity authentication
ISO 20828:2006	Road vehicles - Security certificate management
ISO/TS 21547:2010	Health informatics - Security requirements for archiving of electronic health records - Principles
ISO/IEC 21827:2008	Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)
ISO 22857:2013	Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health data
ISO 24534-4:2010	Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques
ISO 24534-5:2011	Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 5: Secure communications using symmetrical techniques
ISO/IEC TR 24714-1:2008	Information technology - Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General guidance

ISO/IEC TR 24729-4:2009	Information technology - Radio frequency identification for item management - Implementation guidelines - Part 4: Tag data security
ISO/IEC 24759:2014	Information technology - Security techniques - Test requirements for cryptographic modules
ISO/IEC 24760-Parts 1-2:2015	Information technology - Security techniques - A framework for identity management
ISO/IEC 24761:2009	Information technology - Security techniques - Authentication context for biometrics
ISO/IEC 24767-1:2008	Information technology - Home network security - Part 1: Security requirements
ISO/IEC 24767-2:2009	Information technology - Home network security - Part 2: Internal security services: Secure Communication Protocol for Middleware (SCPM)
ISO/IEC 24824-3:2008	Information technology - Generic applications of ASN.1: Fast infoset security
ISO/IEC 27000:2014	Information technology - Security techniques - Information security management systems - Overview and vocabulary
ISO/IEC 27001:2013	Information technology - Security techniques - Information security management systems - Requirements
ISO/IEC 27002:2013	Information technology - Security techniques - Code of practice for information security controls
ISO/IEC 27003:2010	Information technology - Security techniques - Information security management system implementation guidance
ISO/IEC 27004:2009	Information technology - Security techniques - Information security management - Measurement
ISO/IEC 27005:2011	Information technology - Security techniques - Information security risk management
ISO/IEC 27006:2015	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2011	Information technology - Security techniques - Guidelines for information security management systems auditing
ISO/IEC 27010:2015	Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2008	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27014:2013	Information technology - Security techniques - Governance of information security

ISO/IEC TR 27015:2012	Information technology - Security techniques - Information security management guidelines for financial services
ISO/IEC 27017:2015	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2014	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27032:2012	Information technology - Security techniques - Guidelines for cybersecurity
ISO/IEC 27033-1:2015	Information technology - Security techniques - Network security - Part 1: Overview and concepts
ISO/IEC 27033-2:2012	Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3:2010	Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
ISO/IEC 27033-4:2014	Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways
ISO/IEC 27033-5:2013	Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27034-Parts 1-2:2015	Information technology - Security techniques - Application security
ISO/IEC 27035:2011	Information technology - Security techniques - Information security incident management
ISO/IEC 27036-Parts 1-3:2014	Information technology - Security techniques - Information security for supplier relationships
ISO/IEC 27037:2012	Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27039:2015	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)
ISO/IEC 27040:2015	Information technology - Security techniques - Storage security
ISO/IEC 27041:2015	Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27799:2008	Health informatics - Security management in health using ISO/IEC 27002

ISO/IEC 29100:2011	Information technology - Security techniques - Privacy framework
ISO/IEC 29101:2013	Information technology - Security techniques - Privacy architecture framework
ISO/IEC 29147:2014	Information technology - Security techniques - Vulnerability disclosure
ISO/IEC 29167-Parts 1-17:2015	Information technology - Automatic identification and data capture techniques
ISO/IEC 29180:2012	Information technology - Telecommunications and information exchange between systems - Security framework for ubiquitous sensor networks
ISO/IEC 29192-Parts 1-4:2013	Information technology - Security techniques - Lightweight cryptography
ISO/IEC TS 30104:2015	Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements
ISO/IEC 30111:2013	Information technology - Security techniques - Vulnerability handling processes
IEC 80001-1:2010	Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

ÖNORMEN:

A 7700-1	Webapplikationen - Teil 1: Begriffe
A 7700-2	Webapplikationen - Teil 2: Anforderungen durch Datenschutz
A 7700-3	Webapplikationen - Teil 3: Sicherheitstechnische Anforderungen
A 7700-4	Webapplikationen - Teil 4: Anforderungen an den sicheren Betrieb

C.2 Referenzdokumente

Nachfolgend werden die Dokumente angeführt, auf die im vorliegenden Sicherheitshandbuch direkt Bezug genommen wird. Dabei wird generell die Version angegeben, die bei Erstellung des Handbuchs zugrunde gelegt wurde. Da die meisten der nachfolgend angeführten Dokumente regelmäßig oder bei Bedarf aktualisiert werden, empfiehlt es sich, stets auch auf die aktuelle Version eines Dokumentes zu achten.

[AVB-IT]	Allgemeine Vertragsbedingungen der Republik Österreich für IT-Leistungen, verfügbar über die Bundesbeschaffungs GmbH, Version 2015, verfügbar über www.bbg.gv.at. In Anhang B sind beispielhaft Auszüge aus den AVB-IT angeführt.
[BITK10]	BITKOM-Leitfaden-CloudComputing_Web: Cloud Computing – „Was Entscheider wissen müssen“, BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Albrechtstraße 10 A, 10117 Berlin-Mitte, Dr. Mathias Weber, Arbeitskreis Cloud Computing und Outsourcing, www.bitkom.org, 2010
[BSCA10]	BURTON GROUP - “Building a Solid Cloud Adoption Strategy: Success by Design”, Drue Reeves, dreeves@burtongroup.com, Mai 2010
[BSI GSHB], [BSI Standards], [BSI M (Maßnahmenkataloge)]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn: „IT-Grundschutz-Standards“, „IT-Grundschutz-Kompendium“ (vormals IT-Grundschutzkataloge und IT-Grundschutzhandbuch), verfügbar unter www.bsi.bund.de
[CCDS]	Cloud Computing und Datenschutz: T. Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Abgerufen aus dem WWW am 19. Jänner 2016 unter www.datenschutzzentrum.de Cloud Computing
[CLD-KOM]	Cloud Computing Kompass: Eine Orientierungshilfe für Cloud-Service-Kunden, A-SIT Plus GmbH, Version 1.0, Dezember 2017: Cloud Computing Kompass

[Common Criteria]	„Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria, CC); vgl. dazu auch ISO/IEC 15408; Die CC können von verschiedenen Servern und E-Mail-Boxen abgerufen werden, vgl. u. a.: Common Criteria Portal und BSI (D)
[CSC]	Leitfaden Cyber-Sicherheits-Check, BSI, ISACA, Februar 2020: https://www.allianz-fuer-cybersicherheit.de
[DSCC10]	BURTON GROUP - “The Dark Side of Cloud Computing”, Drue Reeves, dreeves@burtongroup.com, Mai 2010
[ENISA12-2016]	Indispensable baseline security requirements for the procurement of secure ICT products and services, ENISA, v.1.0, December 2016, verfügbar auf enisa.europa.eu
[IT-BVM]	„Bundesvorgehensmodell (IT-BVM), Vorgehensmodell für die Entwicklung von IT-Systemen des Bundes“, Version 1.0, April 1999, www.bv-modell.at
[ITSEC]	Commission of the European Communities, Directorate-General XIII: „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“, Amt für Veröffentlichungen der Europäischen Gemeinschaften, Version 1.2 vom Juni 1991, ISBN 92-826-3003-X
[ITSEM]	Commission of the European Communities, Directorate-General XIII: „Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)“, Amt für Veröffentlichungen der Europäischen Gemeinschaften, Version 1.0 vom September 1993, publ. 1994, ISBN 92-826-7078-2
[ITU-T]	International Telecommunications Union (ITU) - Telecommunications Standardization Sector (ITU-T)
[IKT-CLOUD]	Kooperation Bund/Länder/Gemeinden: „Cloud Computing Positionspapier 2016“, Version 1.1.3 vom 07.11.2016, verfügbar über den E-Goverment-Reference-Server

[IKT-CLWLAN] Stabsstelle IKT-Strategie des Bundes: „Checkliste WLAN“, Version 1.0 vom Juni 2004, verfügbar über den E-Goverment-Reference-Server

[IKT-KON] Kooperation Bund/Länder/Gemeinden: Auflistung Konventionen und weiterer Konzepte, verfügbar über den E-Goverment-Reference-Server

[IKT-LDAP] Kooperation Bund/Länder/Gemeinden: „Spezifikation LDAP-gv.at“, Version 2.5.0 vom 28.03.2012, verfügbar über den E-Goverment-Reference-Server

[IKT-PVP] Kooperation Bund/Länder/Gemeinden: „Portal Verbund Whitepaper“, Version 2.0 vom Oktober 2007, verfügbar über den E-Goverment-Reference-Server

[IKT-SZERT] Stabsstelle IKT-Strategie des Bundes: „Richtlinien für Serverzertifikate“, aktuelle Version im BKA-Wiki

[IKT-WLAN] Bundeskanzleramt, IT-Koordination: „Beachtens- und Wissenswertes zu WLANs in der Verwaltung“, Version 1.3 vom Mai 2003, verfügbar über www.bka.gv.at

[IKT-ZERT] Bundeskanzleramt, IT-Koordination: „Object Identifier der öffentlichen Verwaltung“, OID-T1 und OID-T2, Version 1.0.0 bzw. 1.0.3, verfügbar über den E-Goverment-Reference-Server

[K-Fall] Bundeskanzleramt: „Katastrophenvorsorge- und Ausfallssicherheitsüberlegungen im IT-Bereich“, vom Oktober 2002

[KIT S04] Bundeskanzleramt, IT-Koordination: „Richtlinien des Fachausschusses für Netzwerke der KIT zur gesicherten Anbindung an Fremdnetzwerke“ („AFNW-Richtlinien“), Version vom 01.09.2000, verfügbar über das ISK

[LCCR] Leitfaden Cloud Computing Recht, Datenschutz & Compliance: EuroCloud Deutschland_eco e. V., 22-27. abrufbar unter www.eurocloud.de

[NSA-SD7] National Security Agency (NSA) - System and Network Attack Center (SNAC), The 60 Minute Network Security Guide, Mai 2006

[OESCS] Österreichische Strategie für Cybersicherheit 2021 (ÖSCS 2021), Dezember 2021, verfügbar über www.bundeskanzleramt.gv.at

[PCEC09] BURTON GROUP - Planning Considerations for Externalization and Cloud Computing, Mike Rollings, mrollings@burtongroup.com, Oktober 2009

D Referenztabellen

Version 3.1.5 nach Version 4.x

> *Zu beachten ist, dass die Kapitelstruktur der Version 4.0 zwar der Struktur von ISO/IEC 27001/27002 angenähert ist, die Kapitel aber nicht ident sind.*

Die folgende PDF-Datei enthält eine Gegenüberstellung des Sicherheitshandbuchs in der Version 3.1.5, welche sich an der Norm ISO/IEC 27001:2005 orientiert, und der Version 4.0, die sich an der ISO/IEC 27001:2013 orientiert. Referenztabelle als PDF

E Referenzierte IKT-Board-Beschlüsse und Gesetze

IKT-Board-Beschlüsse

Nachfolgend sind die im Rahmen des Sicherheitshandbuchs referenzierten IKT-Board-Beschlüsse aufgelistet und zusammengefasst. Die Beschlüsse sind mittlerweile in die Jahre gekommen und bilden teilweise aufgrund geänderter technischer Details inhaltlich nichtmehr den Stand der Technik ab. Sie wurden jedoch der Vollständigkeit halber und um die Nachvollziehbarkeit zu gewährleisten als Referenz beibehalten.

Die Kurzbeschreibung beschreibt nur den Kern des Themas, um die zu Grunde liegende IKT-Board-Entscheidung leichter identifizieren zu können. Nähere Informationen zu den Beschlüssen sind unter folgender Post- bzw. E-Mail-Adresse erhältlich:

Bundeskanzleramt
Bereich IKT-Strategie des Bundes
Ballhausplatz 2
A-1014 Wien
i11@bka.gv.at

Referenz	Sitzungsdatum	Beschreibung
[IKTB-260701-1]	26.07.2001	Beschluss zu Single Sign-On
[IKTB-040901-1]	04.09.2001	Security Layer
[IKTB-140102-1]	14.01.2002	e-card/Dienstkarte
[IKTB-040402-2]	04.04.2002	PKI–Zertifikate
[IKTB-040402-3]	04.04.2002	Portalverbund
[IKTB-250602-1]	25.06.2002	Open-Source/Linux (Ausschreibungsbedingung)
[IKTB-170902-4]	17.09.2002	Ausweichsysteme

Referenz	Sitzungsdatum	Beschreibung
[IKTB-170902-7]	17.09.2002	Vertrauen in Betriebssysteme (Initialkonfiguration)
[IKTB-170902-8]	17.09.2002	Sicherheitspolicies der Ressorts
[IKTB-051102-1]	05.11.2002	Ciphersuites und Keystores im Portalverbund
[IKTB-181202-1]	18.12.2002	Zertifikate
[IKTB-110303-1]	11.03.2003	Kennzeichnung von Sicherheitszertifikaten (Servererkennung)
[IKTB-110303-2]	11.03.2003	Verwaltungskennzeichen
[IKTB-110903-3]	11.09.2003	Einsatz von PKI
[IKTB-281003-19]	28.10.2003	Serverzertifikate – Allgemeine Richtlinien
[IKTB-161203-01]	16.12.2003	Vertrauliche und ausfallsichere Kommunikation
[IKTB-090204-03]	16.12.2004	Amtssiegel
[IKTB-240304-01]	24.03.2004	Portalverbund und portal.gv.at
[IKTB-110504-01]	11.05.2004	Domänenpolicy
[IKTB-230904-01]	23.09.2004	Elektronischer Bescheid
[IKTB-030505-01]	23.09.2004	Zertifikate im Rahmen der Bundesverwaltung

Gesetzestexte

Die zitierten Gesetzestexte und deren aktuelle Fassungen können online über das Rechtsinformationssystem des Bundes unter folgender URL abgerufen werden:

https://www.ris.bka.gv.at/

[AschG]	ArbeitnehmerInnenschutzgesetz (AschG), Stammfassung: BGBl-Nr. 450/1994
[B-BSG]	Bundes-Bedienstetenschutzgesetz (B-BSG), Stammfassung: BGBl-Nr. 70/1999
[DSG]	„Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (Datenschutzgesetz – DSG), Stammfassung: BGBl. I Nr. 165/1999
[DSGVO]	„Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ (Datenschutz-Grundverordnung - DSGVO)
[E-GovG]	„Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen“ (E-Government-Gesetz - E-GovG), Stammfassung: BGBl. I Nr. 10/2004
[EU 5775/01]	„Beschluss des Rates über die Annahme der Sicherheitsvorschriften des Rates“, 07.03.2001
[EU 1999/93/EG]	„Richtlinie 1999/93/EG des europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“
[eIDAS-VO]	„Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ (eIDAS-VO)
[SigV]	„Verordnung des Bundeskanzlers über elektronische Signaturen“ (Signaturverordnung 2008 - SigV), Stammfassung: BGBl. II Nr. 3/2008
[SVG]	„Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen“ (Signatur- und Vertrauensdienstegesetz – SVG), Stammfassung: BGBl. I Nr. 50/2016

[SVV]	„Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen“ (Signatur- und Vertrauensdiensteverordnung – SVV), Stammfassung: BGBl. II Nr. 208/2016
[GTelG]	„Bundesgesetz betreffend Datensicherheitsmaßnahmen beim elektronischen Verkehr mit Gesundheitsdaten und Einrichtung eines Informationsmanagement“ (Gesundheitstelematikgesetz - GTelG), Stammfassung: BGBl. I Nr. 179/2004
[TKG]	Telekommunikationsgesetz, Stammfassung: BGBl. I Nr. 100/1997
[InfoSiG]	„Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen“ (Informationssicherheitsgesetz, InfoSiG), Stammfassung: BGBl. I Nr. 23/2002
[NIS-RL]	„Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ (NIS-RL)
[NISG]	„Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)“, Stammfassung: BGBl. I Nr. 111/2018
[NISV]	„Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz“ (Netz- und Informationssystemsicherheitsverordnung – NISV), Stammfassung: BGBl. II Nr. 215/2019
[QuaSteV]	„Verordnung des Bundesministers für Inneres zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz“ (Verordnung über qualifizierte Stellen – QuaSteV), Stammfassung: BGBl. II Nr. 226/2019

[V A-SIT]	Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie - Austria (A-SIT)“ als Bestätigungsstelle, BGBl. II Nr. 31/2000
[VBG]	Bundesgesetz über das Dienst- und Besoldungsrecht der Vertragsbediensteten des Bundes (Vertragsbedienstetengesetz 1948 - VBG), Stammfassung: BGBl. Nr. 86/1948
[BDG 1979]	Bundesgesetz über das Dienstrecht der Beamten (Beamten-Dienstrechtsgesetz 1979 - BDG 1979), Stammfassung: BGBl. Nr. 333/1979
[RDG]	Bundesgesetz über das Dienstverhältnis der Richter und Richteramtsanwärter (Richterdienstgesetz - RDG), Stammfassung: BGBl. Nr. 305/1961
[ArbVG]	Bundesgesetz betreffend die Arbeitsverfassung (Arbeitsverfassungsgesetz - ArbVG), Stammfassung: BGBl. Nr. 22/1974
[AußHG]	Bundesgesetz über die Durchführung des Warenverkehrs der Ein- und Ausfuhr (Außenhandelsgesetz 1995 - AußHG 1995), Stammfassung: BGBl. Nr. 172/1995
[PVG]	Bundesgesetz über die Personalvertretung bei den Dienststellen des Bundes (Bundes-Personalvertretungsgesetz - PVG), Stammfassung: BGBl. Nr. 133/1967
[Urheberrechtsgesetz]	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), Stammfassung: BGBl. Nr. 111/1936
[HalonbankV]	Verordnung über die Einrichtung einer Halonbank (Halonbankverordnung - HalonbankV), BGBl. II Nr. 77/2000
[Halonverbot]	Verordnung über das Verbot von Halonen, BGBl. Nr. 576/1990
[StGB]	Bundesgesetz über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB), Stammfassung: BGBl. Nr. 60/1974

F Wichtige Adressen

Die angegebenen Adressen entsprechen dem Stand zum Zeitpunkt des Redaktionsschlusses des vorliegenden Handbuchs. Dabei ist zu beachten, dass insbesondere Internetadressen einer besonderen Dynamik unterliegen.

Österreich:

Bundeskanzleramt, Büro der Informationssicherheitskommission (ISK)
Ballhausplatz 2
A-1014 Wien
Tel.: 01 531 15 202594
isk@bka.gv.at

Österreichische Datenschutzbehörde (DSB)
Barichgasse 40-42
A-1030 Wien
Tel.: 01 521 520
www.dsb.gv.at

Austrian Standards Institute (Österreichisches Normungsinstitut, ON)
Heinestraße 38
A-1020 Wien
Tel.: 01 21300
www.austrian-standards.at

Rundfunk und Telekom Regulierungs-GmbH (RTR)
Mariahilfer Straße 77-79
A-1060 Wien
Tel.: 01 580580
www.rtr.at

Verband der Sicherheitsunternehmen Österreichs (VSÖ)
Müllnergasse 4/10
A-1090 Wien
Tel.: 01 3194132
www.vsoe.at

Verband der Versicherungsunternehmen Österreichs (VVÖ)
Schwarzenbergplatz 7
A-1030 Wien
Tel.: 01 711560

www.vvo.at

Zentrum für sichere Informationstechnologie - Austria (A-SIT)
Seidlgasse 22/9
A-1030 Wien
Tel.: 01 503 19630
www.a-sit.at

International:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
D-53175 Bonn
www.bsi.bund.de

International Organisation for Standardisation (ISO)
1, ch. de la Voie-Creuse
Case postale 56
CH-1211 Genève 20
www.iso.org

VdS Schadenverhütung
Amsterdamer Straße 174
D-50735 Köln
Tel. 0049 221 7766 0
www.vds.de