Österreichisches Informationssicherheitshandbuch - Cloud Strategie

Version 3.1
03.12.2012

BUNDESKANZLERAMT ÖSTERREICH

Inhalt

A.3 Cloud Computing

Dieser Anhang soll Grundlageninformationen für nötige strategische Entscheidungen zum Thema Cloud Computing bereitstellen bzw. wie man diese Entscheidungsgrundlagen erarbeitet und was man dabei beachten muss. Es beinhaltet Begriffsdefinition, Marktsituation, rechtliche/strukturelle/wirtschaftliche/ technische Aspekte (Geschäftsprozesse), Auswirkungen, Chancen und Risiken sowie potentielle Anwendungen für klassische Rechenzentren, eine Private Cloud und Public Cloud als auch Beispiele und Prozesse für Migration.

Einleitung

Cloud Computing ist eine Form der flexibel am Ressourcenbedarf orientierten Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bzw. Intranet bereitgestellt und nach Nutzung abgerechnet. Die Nutzer (also die internen IKT-Dienstleister der öffentlichen Verwaltung) 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 Einsatz von Mitteln und eine Umverteilung von Investitions- zu Betriebsaufwand. Beides kann somit 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.

Cloud Computing ist eine Chance, birgt aber auch Risiken. Das hier vorliegende Kapitel beruht auf einem von der Plattform Digitales Österreich erstellten Positionspapier und soll Grundlageninformationen für nötige strategische Entscheidungen bereitstellen bzw. wie man diese Entscheidungsgrundlagen erarbeitet und welche grundlegenden Dinge zu beachten wären. Es beinhaltet Begriffsdefinition, Marktsituation, rechtliche/strukturelle/wirtschaftliche/technische Aspekte (Geschäftsprozesse), Auswirkungen, Chancen und Risiken sowie potentielle Anwendungen für klassische Rechenzentren, eine Private Cloud und Public Cloud als auch Beispiele und Prozesse für Migration.

A.3.1 Begriffsdefinition

Cloud Computing ist ein Begriff, der bereits seit ein paar Jahren die IT-Landschaft prägt. Dahinter verbergen sich zum Teil zwar altbekannte Architekturen und Konzepte, die aber Dank fortschreitender technischer Entwicklungen erstmals markttauglich umsetzbar sind. Einer der Schlüsselaspekte hinter dem breiten Interesse an Cloud Computing ist eine mögliche wirtschaftliche Effizienzsteigerung gegenüber traditionellen IT Verfahren. Dem zur Seite stehen Begriffe wie Kunden / Nutzer / Auftraggeber / Anwender, Organisation, IT-Organisation wobei im Zusammenhang mit Cloud Computing folgendes damit verstanden werden soll: Kunde - der gegenüber dem Cloud Service Provider (CSP) oder auch Cloud Anbieter auftretende Auftraggeber – Ein Beispiel auf Ebene des Bundes wäre z.B. Ministerium.

Hinter Cloud Computing steht ganz allgemein das Anbieten bzw. Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden. Charakteristisch ist des Weiteren, dass Ressourcen oder Dienste nicht unbedingt dediziert einem Kunden zugeordnet, sondern auch dynamisch je nach Bedarf – und Vertragsmodell – zur Verfügung gestellt werden (shared services/resources).

Grob zusammengefasst versteht man darunter eine bedarfsgerechte und flexible Bereitstellung von IT-Ressourcen, deren tatsächliche Nutzung abgerechnet wird.

Das National Institute of Standards and Technology (NIST) kategorisiert Cloud Computing-Dienste anhand von Charakteristiken, Servicemodellen sowie Einsatzvarianten (vgl. [NIST09]).

A.3.1.1 Charakteristiken von Cloud Computing

- **On-Demand Self-Service / Self-provisioning of resources**
  (Ressourcenmanagement durch Nutzer/Kunde)
  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 Service Provider 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, PDAs oder Smartphones ermöglichen.
- **Resource Pooling**
  Die Rechenressourcen des Providers 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 unbeschränkt Ressourcen zur Verfügung, die jederzeit und in jedem Umfang gekauft bzw. genutzt werden können. Dank der dynamischen Verteilung von Ressourcen und Diensten können 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.

A.3.1.2 Servicemodelle des Cloud Computings

Im Zusammenhang mit Cloud Computing existiert eine Klassifizierung der Services in drei unterschiedliche Modelle – eine Detaillierung bzw. Zuordnung ist in den folgenden Kapiteln nach Möglichkeit durchgeführt worden bzw. ist spätestens zum Zeitpunkt einer Überlegung der Nutzung in der Analyse des Services / der Anwendung anzustellen:

- **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.

Zusätzlich werden aktuell weitere Ebenen diskutiert:

- **Business Process as a Service (BPaaS):**
  geht aus der SaaS-Ebene hervor und wird durch eine stärkere Nähe zum Geschäftsprozess charakterisiert.
- **Data as a Service (DaaS)**
- **Network as a Service (NaaS)**

A.3.1.3 Ausprägungen von Cloud Computing

In der Praxis sind drei grundsätzliche Ausprägungen für Cloud Computing zu unterscheiden – die Unterscheidung wird nach Möglichkeit in den folgenden Kapiteln angewandt. Sollte keine Unterscheidung angegeben sein, wäre trotzdem zum Zeitpunkt der Überlegung der Nutzung von Cloud Ausprägungen die Unterscheidung individuell anzuwenden bzw. hinsichtlich der Chancen und Risken zu analysieren:

- **Public Cloud:** Die Cloud-Infrastruktur ist öffentlich über Internettechnologien zugänglich und wird von einem CSP betrieben. 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:** ist eine spezifische Public Cloud Ausprägung, wobei mittels geeigneter Sicherheitsvorkehrungen dem Kunden eine abgekapselte IT-Infrastruktur zur Verfügung gestellt wird, die unter Verwendung von Secure VPN (Virtual Private Network) Technologie direkt mit dem Kunden-Netzwerk verbunden ist.
- **Private Cloud:** Die Cloud-Infrastruktur wird für einen einzelnen Auftraggeber bzw. vorgegebene Gruppe betrieben, die ausschließlichen Zugriff auf die Cloud hat. Sie kann die Infrastruktur selbst oder durch Dritte betreiben lassen. Skaleneffekte und Kosteneinsparungen werden reduziert, stärkere Individualisierungen der Dienste (d.h. Anpassung auf die Erfordernisse der Kunden) sind 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.

Zusätzlich kommen in der Literatur weitere Begriffe wie Enterprise Cloud, Exclusive Cloud, etc. vor. Diese lassen sich aber aufgrund deren Eigenschaften immer einer dieser drei Hauptmodelle unterordnen. Das der Cloud zu Grunde liegende Netzwerk ist in der Regel offen (bei Public Clouds ist dies meist das Internet). Selbst die in einer Cloud zur Verfügung gestellten Ressourcen und Dienste konzentrieren sich nicht auf einzelne, wenige Standorte. Vielmehr können die in einer Cloud angebotenen Dienste und Ressourcen global verteilt sein. Ein CSP entspricht daher nicht mehr zwingend dem Bild eines klassischen Rechenzentrumsbetreibers mit wenigen, überschaubaren Standorten (dies gilt insbesondere bei Public Clouds).

A.3.2 Rechtliche Aspekte/Auswirkungen/Chancen/Risiken

Aus rechtlicher Sicht betrifft Cloud Computing mehrere Rechtsgebeite [CCDS]

A.3.2.1 Grundsätzliches

Folgende Gebiete sind von besonderer Bedeutung:

- Datenschutzrecht
- Vergaberecht
- IT-Vertragsrecht
- Haftung und Gewährleistung
- Strafprozessrecht

Wie bei allen Outsourcing Modellen ist bewusst auch auf Unternehmensveräußerung, Konkurs und Liquidation sowie Zugriff auf die 'eigenen Daten' im Detail rechtlich einzugehen.

A.3.2.2 Datenschutzrecht

Werden personenbezogene Daten in einer Cloud verarbeitet, so ist die Bedeutung des Datenschutzrechts zentral. Der Auftraggeber hat bei der Auswahl seines Dienstleisters die freie Wahl, jedoch muss dieser die auch die Dienstleisterpflichten einhalten. Der Auftraggeber hat weiters seine Auftraggeberpflichten einzuhalten bzw. sicherzustellen, dass sein Dienstleister dies tut. Die Verantwortung für die Einhaltung dieser Auftraggeber- und Dienstleisterpflichten verbleibt jedoch letztlich beim Auftraggeber. Im Einzelfall kann die Abgrenzung der Rolle des Auftraggebers und des Dienstleisters schwierig sein. Im Zweifel ist jedoch anzunehmen, dass die Behörde als Auftraggeber angesehen wird.

Grundsätzlich zählt es zu den Pflichten auch des Dienstleisters die erforderlichen Datensicherheitsmaßnahmen des § 14 DSG (z.B. Schutz vor zufälliger und unrechtmäßiger Zerstörung, Verlust oder unbefugtem Zugriff auf die Daten, Protokollierung der Zugriffe) und das Datengeheimnis gem. § 15 DSG einzuhalten. Weiters sind die Betroffenenrechte (Auskunfts-, Richtigstellungs-, Löschungs- und Widerspruchrecht gem. §§ 26-28 DSG) einzuhalten. Bei verteilten Ressourcen wie dies bei Clouds üblich ist, kann die Einhaltung dieser Datenschutzanforderungen allerdings eine Herausforderung darstellen.

Sofern eine Überlassung der Daten ins Ausland erfolgt, ist diese nur innerhalb des Europäischen Wirtschaftsraum genehmigungsfrei (§ 12 DSG). Ansonsten besteht eine Genehmigungspflicht durch die Datenschutzkommission (§ 13 DSG), die eine Genehmigung nur dann zu erteilen hat, wenn der ausländische Dienstleister die schriftliche Zusage macht, die Dienstleisterpflichten des § 11 DSG einzuhalten. Gerade die verteilte Architektur von Clouds, die sich über mehrere und verschiedene Territorien erstrecken und demnach auch unterschiedlichen Datenschutzrechtssystemen unterworfen bzw. nicht verpflichtet sind das EU-Datenschutzrecht einzuhalten, bereitet Schwierigkeiten. Zwar hat die EU die Datenschutzbestimmungen auch einiger Nicht-Mitgliedstaaten als gleichwertig eingestuft, jedoch deckt dies nicht alle Staaten ab und ist stets im Einzelfall zu prüfen (viele Public Cloud Angebote kommen von US Firmen, daher sind die EU-US Bestimmungen in diesem Bereich vermutlich von hoher Bedeutung). Darüber hinaus können Einzelsysteme oder ganze Clouds auch außerhalb nationaler Territorien (z.B. auf Hochsee, sog. „off-shoring“) betrieben werden, wo jeglicher rechtlicher Datenschutz fehlt [EGCC10]. Zwar kann versucht werden die Datenschutzverpflichtungen vertraglich dem Cloud-Betreiber zu überbinden, jedoch können dadurch (derzeit) widersprüchliche gesetzliche Regelungen des Cloud-Standorts nicht abgeändert werden. So können beispielsweise umfassende Zugriffsrechte von ausländischen Behörden auf die Daten bestehen, die dem europäischen und österreichischen Datenschutzgedanken widersprechen

[EGCC10]. Da noch nicht absehbar ist, in welche Richtung sich die Entwicklung der europäischen Gesetze gestaltet, sei auf die Beachtung der dynamischen Entwicklung dieser Gesetze hingewiesen, die vor allem auch für die Umsetzung der europäischen Digitalen Agenda (Digital Single Market) erfolgen wird.

Folgende Sammlung von Basisfragen [EGCC10] gibt einen guten Überblick hinsichtlich der datenschutzrechtlichen Anforderungen:

- Zugriff auf Daten (Access):
  Die Person, auf die sich Daten beziehen (d.h. der/die Betroffene im Sinne des DSG), kann sowohl Auskunft über, als auch Korrektur oder das Löschen dieser Daten verlangen. Es ist daher darauf zu achten, dass sowohl Einsichtnahme als auch das Löschen in der Cloud gemäß der rechtlichen Vorgaben gewährleistet wird.
- Speicherort von Daten (Storage):
  Bestimmte Datenschutzbestimmungen verbieten den Transfer von Daten in andere oder bestimmte Länder, oder es ist die explizite Zustimmung durch jene Person, auf die sich die Daten beziehen, erforderlich. Es ist daher abzuklären wo die Daten (bzw. auch deren Backup) gespeichert werden und wie sie sich verteilen können, da bspw. im Zuge einer dynamischen Umverteilung Land/Ort der Datenspeicherung wechselt.
- Verbleib von Daten (Retention):
  Daten werden in der Regel im Auftrag des Nutzers in der Cloud gehalten. Es ist zu klären ob der Cloud Service Provider unter einer definierten Retention-Policy arbeitet und wie lange Daten (u.A. auch Verkehrs- und Metadaten) gespeichert werden.
- Vernichten von Daten (Destruction):
  Am Ende der Haltezeit von Daten müssen diese geeignet gelöscht werden. Dementsprechend ist zu klären, ob der Cloud Service Provider, und wenn ja, welche Policy der Betreiber zum Löschen von Daten betreibt. Es ist zu klären welche Verfahren eingesetzt werden und ob diese auch garantieren, dass die betreffenden Daten tatsächlich im Sinne des DSG gelöscht sind und wie mit den Datenträgern verfahren wird. Dies betrifft ebenfalls die Backup-Daten.
- Datenschutzkonformität (Compliance):
  Es sind die Datenschutzbestimmungen im System (bzw. auch die der Einzelsysteme der Cloud) abzuklären und abzustimmen.
- Audit und Monitoring (Audit/Monitoring):
  Es ist sicherzustellen, dass der Auftraggeber (Nutzer) der Cloud die Einhaltung der Datenschutzbestimmungen durch den Cloud Service Provider auditieren und monitoren kann.
- Datenschutzverletzungen (Privacy Breaches):
  Es gilt abzuklären ob der Cloud Service Provider nach einer definierten Incident Handling Procedure vorgeht, und ob diese auch Datenschutzverletzungen abdeckt.

Das Auswahlverfahren des Cloud Service Provider sollte die oben genannte Punkte miteinbeziehen. Eine einmalige vertragliche Überbindung an einen Dienstleister ist dabei nicht als ausreichend anzusehen, sondern muss laufend auditiert werden.

Als Besonderheit gilt das Auftreten einer Behörde (im Zuge des E-Government) als Auftraggeber, da die Verantwortung für die Eihaltung der datenschutzrechtlichen Datensicherheitsmaßnahmen die Behörde trägt und daher bei der Auswahl des Cloud-Providers entsprechend vorzugehen ist.

Es ist derzeit anzunehmen, dass die Anforderungen bei Public Clouds, die sich nicht oder nicht nur im (EU-)Inland befinden, kaum zu erfüllen seien bzw. sind in einem Assessment genau zu detaillieren.

A.3.2.3 Vertragsrecht, Haftung und Gewährleistung

Zur Sicherstellung insbesondere auch der datenschutzrechtlichen Anforderungen ist ein auf den Einzelfall abgestimmtes Vertragswerk erforderlich (vertragliche Zusicherung der Einhaltung der datenschutzrechtlichen Anforderungen, SLA, Vereinbarung von z.B. ISO 27001). Da bei Clouds oftmals mehrere Dienstleister bzw. Sub-Dienstleister in Anspruch genommen werden, ist darauf zu achten, mit wem die Dienstleistervereinbarung abgeschlossen wird bzw. ob nicht mehrere Dienstleistervereinbarungen abgeschlossen werden müssen. Darin müssen natürlich auch je nach Typ der Leistung (Leihe, Miete, Werk oder Dienstleistung) die Haftung und Gewährleistungsansprüche geregelt werden, soweit diese im Lichte der Amtshaftung überhaupt disponibel sind. Für den Fall des Betreiberwechsels oder im Insolvenzfall sollten migrierbare (Daten-)Standards vereinbart werden.
Eine gute Aufgliederung notwendiger vertraglicher Regelungen (auch) über die datenschutzrechtlichen Punkte hinaus findet sich etwa unter [LCCR] bzw. [BITK10].

A.3.2.4 Vergaberecht

Obwohl eben aufgrund insbesondere datenschutzrechtlicher Anforderungen der Bedarf eines hohen Individualisierungsgrades des Vertrages besteht, erscheinen abweichende Regelung von den AGB der CSP (mangelnde Zugriffs- und Kontrollrechte, benachteiligende Haftung) schwierig. CSP stellen ihre Leistung zumeist lediglich unter ihren Standard-AGB zur Verfügung.

A.3.2.5 Strafprozessrecht

Aber auch innerstaatliche Auskunftspflichten von Verkehrsdaten (Zugriffsprotokolle) gegenüber österreichischen Behörden in den Bereichen Strafverfolgung und Vorratsdatenspeicherung führen zu besonderen Anforderungen.

A.3.2.6 Sonderprobleme

Im Extremfall können auch Regelungen bestehen, Daten ausschließlich im Inland zu speichern (z.B. im Zusammenhang mit der umfassenden Landesverteidigung), was Clouds außerhalb Österreichs kategorisch ausschließt.

A.3.3 Strukturelle Aspekte/Auswirkungen/Chancen/ Risiken

Im folgenden Abschnitt werden die Chancen, Risken aus der organisatorischen Perspektive dargestellt die Auswirkungen des Cloud Computing auf die IT-Organisation erläutert. Hierbei steht das Modell „Public Cloud“ im Fokus der Betrachtung. Wesentliche Teile der Überlegungen gelten jedoch auch für Private Clouds und Community Clouds.

A.3.3.1 Grundsätzliches

Neben den - im folgenden Abschnitt betrachteten - wirtschaftlichen Vorteilen durch Senkung von Betriebskosten kann Cloud Computing durch deren Merkmale (Standardisierung, …) auch organisatorische Vorteile bieten. Jedoch sind hiermit verbundene Risiken zu beachten. Diese inkludieren die erschwerte Steuerung des IT-Einsatzes, strukturelle Abhängigkeit aufgrund von Lock-in-Effekten gegenüber Cloud-Anbietern sowie der Einhaltung von Governance-Regeln [DSCC10].

Cloud Computing stellt insbesondere die organisatorische Steuerung der IT vor eine Vielzahl von Herausforderungen. Die Gründe hierfür sind:

- Die Entwicklung des Verarbeitungsvolumens: Cloud Computing verspricht – neben der schnellen Provisionierung von Services – Kostensenkungen. In der Praxis kann es aber aufgrund höherer Verbrauchsmengen bei diesem Modell schnell zu unerwartet hohen Kosten kommen.
- Organisatorische Disintegration: Cloud Computing kann bei Anwendung eines ad-hoc Ansatzes zu „Silo-Lösungen“ führen. Der Datenaustausch zwischen Anwendungen kann sich als schwierig erweisen. Die Service-Qualität reduziert sich somit aus der Perspektive des Auftraggebers.
- Unzureichendes Wissen über interne Kosten: Ein objektiver Vergleich der Kosten zwischen einer Cloud-Lösung und einer internen Lösung ist oftmals nicht möglich.

- Strukturelle Abhängigkeit gegenüber Anbietern von Cloud-Lösungen (man muss im Detail unterscheiden zwischen IaaS, PaaS und SaaS): Cloud Computing verspricht Kostensenkungen bzw. höhere Servicequalität aufgrund des Wettbewerbs zwischen den Anbietern dieser Lösung. Der Wettbewerb ist jedoch nur bei herstellerunabhängigen Standards gewährleistet. Diese Standards sind derzeit jedoch noch nicht existent.

Um die Risiken des Cloud Computing zu minimieren bzw. die Potentiale bestmöglich auszuschöpfen, ist die Verwendung eines Vorgehensmodells zur Einführung von Cloud Computing essentiell [PCEC09]. Als Beispiel sei das fünf-stufige Vorgehensmodell von Reeves und Santos genannt [BSCA10]:

- Projektvorbereitung: Formierung eines Kernteams zur Entwicklung einer Cloud-Strategie, Definition von Geschäftszielen und Darlegung der Migrationsgrundsätze, Entwicklung einer Migrations-Roadmap.
- Analyse des Geschäftsfeldes sowie der bestehenden IT-Anwendungen: Identifizierung der Risken und der Einflüsse im Falle eines Ausfalls der Cloud, Analyse der Anforderungen und Abhängigkeiten der IT-Anwendungen, Kostenvergleich Cloud vs. „interner“ 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, Hardware as a Service, Infrastructure as a Service) bzw. der Ausprägung (Private, Public oder Hybrid).
- Auswahl des Cloud-Anbieters: Analyse des Leistungsvermögens sowie des Risikopotenzials der Cloud-Anbieter anhand der ermittelten Anforderungen, Auswahl von geeigneten Evaluierungsverfahren.
- Vermeidung bzw. Reduzierung der Risiken durch Planung einer Exit-Strategie (Vertragsgestaltung, Verwendung offener Datenformate)
- Planung des laufenden Betriebes: Erarbeitung von Governance-Regeln (Management von unerwarteten Ausgaben, Budgetplanung, ungeplante Auswirkungen).

Von **zentraler Bedeutung** ist hierbei die **Analyse der „Cloud-Fähigkeit“** von IT-Anwendungen. Aus einer organisatorischen Perspektive sind folgende Aspekte zu berücksichtigen [BSCA10]:

- Kontinuität: Es gilt abzuklären welche Auswirkungen auf die Kontinuität der Geschäftstätigkeit vorherrscht und damit zu bestimmen wann eine IT-Anwendung zu geschäftskritisch ist, um in die Cloud ausgelagert zu werden und wie hoch liegt der Schwellenwert für Ausfallszeiten.
- Informationssicherheit: Es ist festzustelle welche Daten eine IT-Anwendung aufgrund der besonderen Sensitivität disqualifizieren.
- Risikotoleranz: Es ist zu klären welche Risiken für eine Organisation aufgrund von Service-Ausfällen tragbar sind.

- 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 eines Verfahrens in die Cloud ist festzustellen und als Verhältnis den erwarteten Einsparungen gegenüber zu stellen.

Generell gilt es, die Berücksichtigung der Cloudfähigkeit von neuen Applikationen bereits in der Architekturphase einzuplanen.

A.3.4 Wirtschaftliche Aspekte/Auswirkungen/Chancen/ Risiken

A.3.4.1 Grundsätzliches

Die Cloud Service Provider (CSP) realisieren die Kostenvorteile vor allem durch das Standardisieren von Services, das Bündeln von IT-Ressourcen und Automatisierung von Abläufen. Auf Anbieterseite ermöglicht das Cloud-Konzept 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 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.

Cloud Computing bedeutet daher aus wirtschaftlicher Sicht:

- Standardisierte IT-Infrastruktur und –Dienste sind unter den Rahmenbedingungen einer Cloudarchitektur und eines Cloudgeschäftsmodells wirtschaftlicher zu beziehen bzw. zu erbringen. Die Anwendungen sind jedoch umfassend zu betrachten.
- 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 man im Detail unterscheiden 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 für die Verwaltung 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 der Verwaltung 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. Der Private Cloud Anbieter für eine große Organisation selbst muss investieren. Die Zusammenfassung von mehreren internen Kunden in einer Private Cloud bringt 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 1:1 auf eine Mischform bzw. mögliche Private Clouds bzw. Community Clouds der heimischen Verwaltung übertragen werden.

A.3.5 Technische Aspekte/Auswirkungen/Chancen/ Risiken und Sicherheit

Technische Aspekte wie Virtualisierung, Provisioning, gemeinsame Nutzung von Ressourcen und Ausgleichen von Lastspitzen sowie Externalisierung von Investitionskosten sind Grundeigenschaften, die Cloud Computing ausmachen.

A.3.5.1 Technische Aspekte

Bei der Beschreibung von Cloud Computing-Systemen haben sich u.a. folgende technische Aspekte etabliert.

- **Standardisierung**

IT-Anwendungen haben eine Vielzahl von Schnittstellen bzw. unterhalten Schnittstellen zu anderen Anwendungen. Sind diese Schnittstellen standardisiert, ist ein Wechsel eines Anbieters einfacher, da der Anpassungsaufwand gering sein müsste; von einer breiten Standardisierung sind wir allerdings noch weit entfernt - jedenfalls sind Projektaufwände zu kalkulieren.
Chance: Durch standardisierte Cloud-Umgebungen kann sich technisch gesehen ein Wettbewerb etablieren, der den Wechsel zwischen Anbietern einfacher macht. Die Standards der Schnittstellen bilden daher ein wichtiges Kriterium um nicht in eine Abhängigkeit (Lock-In) zu kommen. Für die Standardisierung gibt es bereits eine Reihe von Standards (z.B. SAML, SPML, XACML, LIAF) die durch die Cloud-Anbieter unterstützt werden sollten.

- **Skalierbarkeit**
  Unter Skalierbarkeit versteht man die Anpassbarkeit von Ressourcen an die – sich ändernden - Leistungsanforderungen von Auftraggebern / Kunden auch bei Lastspitzen (z.B. Dienstbeginn, Tagesabschluss, Monatsabschluss, Volkszählung, Wahlvorbereitung, Volksbefragung, ...).
  Chance: ist hier der Lastausgleich über mehrere Kunden oder Mandanten in der Cloud, da die Grundarchitektur dafür geeignet ist. Gleichzeitig kann es zum Risiko werden, wenn nicht ausreichend Ressourcen vorgehalten werden und damit alle Kunden oder Mandanten beeinträchtigt werden.
- **ID- und Rechtemanagement**
  Die Identitäts- und Rechteverwaltung ist wesentlicher Baustein der Zugangskontrolle in Cloud Computing-Systemen. Um die bestehenden Sicherheitsbedenken auszuräumen, ist daher die Lösung des CSP genau zu hinterfragen wie er damit umgeht, dass **fremde Administratoren Zugang zu Unternehmensdaten** haben. Es muss die sichere Identifikation der Kunden der Cloud selbst wie 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. Es sollten generell für die Authentisierung nur starke Verfahren für Kunden und CSP verwendet werden. Die Connectivity zu einem lokalen IDM (Identity Management) des Kunden ist sicherzustellen, da sonst erhebliche Zusatzaufwände und auch Risken entstehen. Das ID- und Rechtemanagement kann auch bei einem Drittanbieter angesiedelt sein.
- **Mandantenfähigkeit**
  Zu den Grundeigenschaften einer Cloud-Architektur zählt die Mandantenfähigkeit. Die sichere Mandantenfähigkeit in der Cloud soll die Partitionierung einer virtualisierten Shared IT Infrastructure ermöglichen, wie sie auch bei Server-Virtualisierung im modernen Rechenzentrum bereits eingesetzt wird. Dadurch ergibt sich die Chance verschiedene Anwendungsszenarien (z.B.: Produktions- und Testbetrieb) abzubilden.
- **Sicherheitsstruktur**

Um die Ressourcen der Kunden oder Mandanten (Daten, Anwendungen, Netze, …) zu schützen, ist eine durchgängige Sicherheitsarchitektur zu implementieren. Da Cloud-Systeme mandantenfähig (multi-tenancy) sein müssen, ist eine sichere Trennung der Ressourcen von Kunden oder Mandanten in der Architektur abgebildet.

- **Cloud Management**
  Um den Betrieb von Cloud-Services zu gewährleisten, sind vom CSP IT-Managementfunktionen und Prozesse anzubieten, die sowohl die Einrichtung wie auch den Betrieb unterstützen. CSPs offerieren für ihre Services Werkzeuge in Form von Webportalen, die die Funktionen zur Verfügung stellen. Typischer Weise sind folgende Funktionen inkludiert:
  - Steuerung von Services - dazu zählen z.B:
    - das Starten
    - Stoppen
    - Neustarten
  - Überwachung von Services - um die Leistungsfähigkeit/Leistungsdaten des CSP zu erheben.
  - Sicherheit von Services - umfassen den sicheren Zugriff auf Services, Transparenz von Zugriff und die sichere Identifikation von Kunden und Administratoren des CSP

  Wünschenswert wären zudem Werkezuge, mit denen die Cloud Ressourcen und die lokalen on-premise Ressourcen gleich verwaltet werden können.
- **Technische Revision**
  CSP müssen zum Durchsetzen von kundenspezifischen Sicherheitspolitiken dafür geeignete Prozesse anbieten. Es muss dem Kunden möglich sein, im Rahmen der Umsetzung seiner Sicherheitspolitik die benötigten Informationen/ Zugriffe auf z.B. LOG-Dateien, Zugriffslisten u.ä zu haben, um die eigene Compliance zu gewährleisten.
- **Patch Management**
  Unter Patch Management wird die Planung und Installation von Patches (Software-Updates) zusammengefasst. Wichtig ist hier, 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 der Verträglichkeit bzw. Kompatibilität von SW-Updates mit kundenspezifischen Anwendungen zu sehen.

A.3.5.2 Zusammenfassung der technischen Aspekte

Tabelle	Chance	Risiken
Standardisierung	Wettbewerb, Wechsel zwischen Anbietern	Ohne Standard Abhänigkeit von den CSP-Anbietern

Tabelle	Chance	Risiken
Skalierbarkeit	Vorstellung nahezu grenzenloser Ressourcen durch 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" duchgeführt werden	-
Cloud Management	Standarddienste (einheitliche Administratorkonsolen) werden durch komfortable Webportale zur Verfügung gestellt.	Einbindung der Werkzeuge an CSPs in kundenspezifischen Prozessen noch nicht erprobt
Technische Revision	-	Auftrennung der kundenspezifischen Daten (Log-Dateien u.ä.) 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, Bedachtnahme auf kundenspezifische Anforderungen.

A.3.5.3 Sicherheit und Technik

- **Anforderungen / Schutzziele**
  Risiken, die bei konventionellen Web-Diensten oder Services entstehen können, sind bei Cloud-Services ebenfalls zu berücksichtigen. Zu erreichende Schutzziele sollen individuell in Abhängigkeit von Klassifizierungsstufen, Datenschutzrichtlinien und rechtlichen Aspekten definiert und in Kraft gesetzt werden. Die Festlegung und Einhaltung dieser organisatorischen und technischen Maßnahmen seitens der Anbieter, Auftraggeber und Nutzer von Cloud-Services trägt zur Gewährleistung der Informationssicherheit bei. Cloud-basierte Dienste müssen wie andere IT-Dienste die Sicherheitsaspekte in Bezug auf Datenschutz, Informationsschutz, Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, … beachten und stehen denselben Bedrohungen gegenüber.
- **Datenschutz**
  Insbesondere im Hinblick darauf, dass die Daten unter Umständen von einem externen Dienstleister verarbeitet werden, der seinen Rechtssitz im Ausland hat, sind spezielle Vereinbarungen erforderlich. Diese Fragestellungen werden im Kapitel Rechtliche Aspekte behandelt.

- **Informationsschutz**
  Die Verarbeitung, Speicherung und Übertragung von Informationen muss derart gestaltet sein, dass die Schutzziele der zugehörigen IKT-Services eingehalten werden. Dabei sind auch die spezifischen Risken zentralisierter Infrastruktur mit zu betrachten.
- **Vertraulichkeit**
  Informationsvertraulichkeit ist dann gegeben, wenn keine unautorisierte Informationsgewinnung möglich ist. Das erfordert die Festlegung von Berechtigungen und Kontrollen der Art, dass sichergestellt ist, dass Subjekte nicht unautorisiert Kenntnis von Informationen erlangen. Das umfasst sowohl gespeicherte Daten, als auch Daten, die über ein Netzwerk übertragen werden. 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. Die Speicherung soll verschlüsselt erfolgen, um technisch das missbräuchliche Lesen von Daten zu verhindern. Dies ist insbesondere bei der Nutzung von Public Cloud erforderlich. Dies benötigt eine Infrastruktur kryptographischer Dienste, ein entsprechendes Schlüsselmanagement, sowie geeignete Kryptographie-Komponenten. Bis zu einer produktionsreifen Entwicklung der Vollverschlüsselung (Berechtigte 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 die Daten verschlüsselt auf einem Speichermedium vorliegen. In den Geschäftsbedingungen der meisten CSP gibt es keine Zusicherungen darüber, wo die Daten gespeichert werden und wie ihre Vertraulichkeit geschützt wird. Häufig ist 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 der virtuellen Server per Zugriff auf die Virtualisierungsschicht durchgeführt werden. Eine größere Anzahl an Personen hat Zugriff auf die virtuellen Maschinen und die zugehörigen Netze, so dass das Risiko des unautorisierten Zugriffs signifikant höher als in traditionellen IT-Umgebungen ist.
  Aus Optimierungsgründen haben CSP die Möglichkeit, Daten und Services auch zu anderen CSP auszulagern. Dadurch entstehen neue Abhängigkeiten und Risiken, die bewertet werden müssen. Die Vertraulichkeit der Daten muss für den gesamten Daten-Lebenszyklus sichergestellt werden: 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 vollständig gelöscht sind (Backupkopien, Replikationen beim Anbieter, etc.).
- **Integrität**

Ein System gewährleistet die Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Die Integrität von Daten, Nachrichten und Informationen bezeichnet deren Unverfälschtheit bzw. Vertrauenswürdigkeit.
Dieses Ziel sollte nicht nur der Cloud-Service selbst erfüllen, sondern auch alle weiteren beteiligten Komponenten eines Cloud Computing-Systems. Der CSP ist für die Integrität des Systems und der Services vollinhaltlich verantwortlich, und soll vertraglich festgehalten werden. Gespeicherte Daten müssen vor nicht autorisierten Manipulationen geschützt werden. Fehler in der System-Konfiguration des Anbieters können zu einer Integritätsverletzung führen.
Die Daten in Cloud Computing-Systemen sollten 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, bedeutet jedoch einen zusätzlichen Kommunikationsaufwand.
Neben der Datenintegrität sind in Cloud-Systemen auch die Softwareintegrität, Konfigurationsintegrität und Nachrichtenintegrität wichtig.

  - **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-Services nur durch autorisierte Personen geändert werden kann. Dies ist in Cloud-Systemen besonders wichtig, da meist eine Cloud-Umgebung 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.

- **Verfügbarkeit**
  Die Verfügbarkeit gibt an, dass Funktionen eines IKT-Services ständig bzw. innerhalb einer vorgegebenen Zeit, die von Service zu Service unterschiedlich sein kann, zur Verfügung stehen. 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.
- **Authentizität**

Authentizität ist die Echtheit, Zuverlässigkeit und Glaubwürdigkeit eines Objekts. Dadurch wird sichergestellt, dass die Herkunft des Objekts zweifelsfrei nachgewiesen werden kann. Eine Möglichkeit für den Nachweis ist die digitale Signatur.
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, Trennung des Datenverkehrs verschiedener Nutzer, Kontrollverlust von Daten etc. Um einen langfristigen Erfolg von Cloud Computing sicherzustellen, ist die Betrachtung kritischer Erfolgsfaktoren, allen voran das Thema 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 – ich kann aber z.B. keine Verschlüsselung zur Anwendung bringen.
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 darüber hinausgehenden 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.

- **Bedrohungen**
  Bedrohungsszenarien betreffen traditionelle IT-Konzepte und Cloud Computing Modelle zu gleichen Teilen. Die hier skizzierten Bedrohungen stellen die häufigsten Gefahren dar, ohne den Anspruch auf Vollständigkeit zu haben. Es muss daher im konkreten Fall eine spezifische Bedrohungsanalyse erstellt werden.
  Bedrohungen werden grob in zwei Punkte eingeteilt: Daten/Informationen und Services. Daten werden nach Informationssicherheitsgesetz (InfoSiG) in Klassifizierungsstufen (unklassifiziert, eingeschränkt, vertraulich, geheim, streng geheim) eingeteilt, und müssen je nach Stufe einer unterschiedlichen Behandlung zugeführt werden. Informationen, welche als z.B. geheim klassifiziert werden, sind von einer Bearbeitung in einer Public Cloud ausgeschlossen, da eine lückenlose Kontrolle des Zugriffs nicht mehr gewährleistet ist. Diese Kontrollen sind besonders im militärischen Bereich unerlässlich.

Services die von einem Cloud-Anbieter angeboten werden (XaaS), unterliegen einer ständigen potentiellen DoS-Gefahr (Denial of Service) sowie der Gefahr des unberechtigten Datenabflusses durch Dritte.
Social Engineering ist eine der größten Gefahren. Nutzer mit Administratorenrechten werden dazu verleitet, Zugangsdaten-, verfahren, o.ä. preiszugeben. Es sind Ansprechpersonen und Prozesse zu definieren, um bei einem Sicherheitsvorfall sowohl strukturierte Abläufe zu haben, als auch Zuständigkeiten abgrenzen zu können.

- **Trennung von verschiedenen Sicherheitsebenen**
  Dokumente welche nach InfoSiG klassifiziert sind, dürfen nur mehr in einer Private Cloud bzw. Community Cloud verarbeitet werden. Hierbei ist besonders zu berücksichtigen, dass die Trennung nur mehr vertraulich und geheim umfasst. Streng geheime Daten nach InfoSiV §9(2) dürfen nur mehr auf nicht vernetzten und abstrahlungsarmen Geräten verarbeitet werden.
- **Standards und Normen**
  Zurzeit sind Cloud-Service-Provider kaum nach einschlägigen Normen zertifiziert (z.B.: ISO2700X, BSI Grundschutz, BASEL III). Bei der Einholung von Angeboten von CSP wäre also auf derartige Zertifizierungen besonders Wert zu legen.

A.3.6 Prozesse (Geschäftsprozesse) - Aspekte / Auswirkungen / Chancen / Risiken / Integration

A.3.6.1 Grundsätzliches

Cloud Computing ist nicht nur ein Thema für die IT-Abteilungen. Dieses neue IT-Betriebsmodell ist eine Herausforderung für die öffentliche Hand bzw. Unternehmen. Durch Cloud Computing kann eine ganzheitliche Änderung von Unternehmensstrategien und -strukturen notwendig werden, postiv ausgedrückt – auch ermöglichen. Dazu gehört beispielsweise festzulegen, wer die Verantwortung für Datensicherheit übernimmt und nach welchen Prozessen IT-Leistungen eingekauft werden. Nutzung bzw. Einsatz von Cloud Computing fordert möglicherweise eine Umverteilung von Rollen und Kompetenzen (abhängig von der bisherigen Rollenverteilung) und etabliert falls notwendig auch ein neues Rollenverständnis. Die Zusammenarbeit von Nutzer-internen Prozessen und von Prozessen des CSP sind in einem Cloud Compliance Regelwerk transparent festzulegen und zu kontrollieren.

Die wesentlichsten strategischen Treiber für Prozessveränderungen durch die Nutzung von Cloud-Services sind:

- Die Standardisierung der IT-Services ist Voraussetzung für das Einführen von Cloud Services. Diese Standardisierung betrifft nicht nur die Funktion der Services sondern auch die Prozesse zwischen Anbietern und Auftraggebern einer Cloud Umsetzung. Cloud Services können das Durchsetzen von Standards effektiv unterstützen, setzen aber auch sehr enge Limits für die Anpassung der IT-Services an Unternehmensprozesse.
- Cloud-Nutzer gewinnen eine größere Wahlfreiheit bei den standardisierbaren Anwendungen und bei den Anbietern, Governance-Prozesse gewinnen an Bedeutung.

Die Nutzung von Cloud Computing bedeutet das Outsourcen von Teilen der eigenen Geschäftsprozesse an einen Dritten. Im Sinne der Aufgabendefinition und –Überwachung wird insbesondere auf die Notwendigkeit des Abschlusses ausreichender Service Level Vereinbarungen (SLAs) und Operations Level Vereinbarungen (OLAs) verwiesen.

A.3.6.2 Strategische Aspekte der Prozessveränderung durch Cloud Computing

- Auswirkungen des Standardisierungsgrades in Public und Private Clouds
    - Einleitend ist festzuhalten, dass Standardisierung an sich der wesentlichste Treiber für Kostenersparnisse hinter dem Cloud Prinzip ist. Cloud Technologien sind nur eine Fortsetzung, ein Werkzeug zur effizienten Umsetzung von Standardisierung.
    - Massiv skalierende Public Clouds unterliegen einem sehr hohen Standardisierungszwang. Geringer skalierende Public Clouds mit bewusstem Design für Anpassungsmöglichkeiten sowie Private Clouds ermöglichen (beschränkte) Optimierung durch Anpassungen an Kundenbedürfnisse. Durch das Maß der Anpassbarkeit wird die Kostenverteilung zwischen IT und Restunternehmen verändert. Die Kostenveränderungen sind aus Gesamtkostensicht zu betrachten.
- Mögliche Beschleunigung von Unternehmensprozessen
    - Die Flexibilisierung der Nutzung von Computing Ressourcen durch Cloud Computing bietet Phantasie für raschere Anpassung von IT-Ressourcen an die Bedürfnisse eines Kunden.
- Governance-Prozesse
    - Dies begründet sich nicht zuletzt durch das beobachtete und in den untersuchten Studien hervorgehobene „Empowerment der Nutzer“: Durch die erheblich niedrige finanzielle Einstiegsschwelle in der Nutzung und der Geschwindigkeit der Einführung von Public Cloud Services besteht die Gefahr einer Profileration von heterogenen Cloud-Services unterschiedlicher Anbieter in den öffentlichen Bereich, die hinsichtlich technischer Sicherheit, Rechtssicherheit und Flexibilität für organisatorische

Veränderungen (Verwaltungsreform u.a.) schwer beherrschbar werden – jedoch gilt auch hier, individuell zwischen IaaS, PaaS und SaaS zu unterscheiden bzw. urteilen. Die Governance-Prozesse sind daher für Public Cloud Services sehr kritisch zu hinterfragen und mit hoher Wahrscheinlichkeit in vielen Bereichen neu zu definieren. Private Clouds bieten den Vorteil der wesentlich einfacheren zentralen Steuerung und der existierenden Erfahrungen aus Cloud-ähnlichen Projekten im Bund und in den Ländern und Gemeinden, wie wohl auch für Private Cloud Services vermehrte Anforderungen an Governance Prozesse entstehen. Die Anforderungen an Governance Prozesse und Richtlinien müssen strikt zwischen „kritischen Services“, die für das Funktionieren des Staates im Zusammenspiel mit Wirtschaft und Bürgerinnen und Bürgern unabdingbar sind und „anderen Services“ unterscheiden

A.3.6.3 Cloud Compliance

Das hohe Maß an Abhängigkeit zwischen Cloud Anbietern und Nutzern und die dadurch verzahnten Prozesse und Verantwortlichkeiten erfordern ein stabiles Regelwerk, das vielfach unter „Cloud Compliance“ [BITK10] zusammengefasst wird. Cloud Compliance bezeichnet daher die nachweisbare Einhaltung von Regeln zur Nutzung oder Bereitstellung von Cloud Computing. Cloud Compliance hat zum Ziel, Transparenz und Sicherheit für alle Anspruchsgruppen (Stakeholder) zu schaffen. Damit schafft Cloud Compliance eine wichtige Basis, um alle Vorteile des Cloud Computings für Anbieter, Nutzer und Provider vollumfänglich nutzbar zu machen.

A.3.6.4 Entscheidungskriterien zur Auswahl von Cloud-affinen Anwendungen und Services

Unbedingt zu beachten ist, dass die Betrachtung der Unternehmensgröße nur einen einzigen Parameter in einer Vielzahl von Entscheidungsparametern darstellt. Anhand der folgenden Grafik soll ein Überblick gegeben werden, der zeigt welche Cloud-Typen welche Kriterien erfüllen.

Abbildung 1: Bewertung der Cloudtypen

Die Integrationsfähigkeit von Cloudservices 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, …) 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

Die Studie „E-Government und Cloud Services“ gibt exemplarisch Anregungen für mögliche Cloud Services im Umfeld öffentlicher Behörden, welche in den folgenden Paragraphen zitiert sind:

- 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 behördeinternen und/oder bürgerorientierten Prozessen (eFormularen)
  - Plattform zum einfachen Erstellen von Web-Applikationen; diese Plattform bindet über einfache Module (APIs) die E-Government Infrastruktur mit ein (z.B. Zustellung, Payment, Bürgerkarte, SZRServices, etc.)
  - Datenbanken
- Software-as-a-Service (SaaS):
  - Desktop-Software der öffentlichen Verwaltung wird als cloudbasierter Dienst angeboten - Zugriff erfolgt bspw. über Web-Browser
  - Workflow Managment System, wie bspw. elektronische Aktensysteme
  - Collaboration Suite
  - *Identity-Management-as-a-Service*: die Bürgerkartenanmeldung wird nach dem Muster eines Identity Providers als "zentrale" Infrastruktur angeobten.
  - *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 Services, die in eine Cloud-Form migriert werden können

Völlig generell spiegeln die vier Bestimmungsfaktoren-Gruppen für das Outsourcing von Leistungen

- rechtliche Aspekte (siehe dazu Kapitel 2)
- (wirtschafltiche) Verfügbarkeit
- Steuerbarkeit
- Risikobereitschaft

die Gestaltungs- bzw. Handlungsebenen wieder, die für Entscheidungen über die Nutzung von Cloud Computing relevant sind.

Unter Berücksichtigung dieser generellen Grundsätze und der diskutierten Vor- und Nachteile von Cloud-Services bietet sich die Entscheidungsmatrix für die Erprobung und Adoption von Cloud-Services im öffentlichen Dienst an.

Zum Beispiel sind IaaS und PaaS für Test- und Entwicklungsserver sowohl für Private wie 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.

Vertikale Services mit Cloud Potential bzw. mit bereits Cloud-ähnlicher Realisierung wie SAP HV oder SAP PV können auf ihre technische Realisierung hin reviewed werden: Sind alle technischen Trends moderner Cloud Services sinnvoll aufgenommen?

Horizontale branchenunabhängige Service Kandidaten bedürfen der Evaluierung auf Integrationsbedarf, um bestehende Service-Integrationen und Prozessoptimierungen nicht zu verlieren und sie bedürfen einer politischen Willensbildung, ob sie „betriebskritisch“ für die jeweilige Behörde 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

A.3.7.1 Grundsätzliches

Bevor man eine Entscheidung für die Nutzung von Cloud Computing trifft oder ein spezielles Modell auswählt, müssen Grundlagen geschaffen werden. In diesem Zusammenhang sind jedenfalls folgende Punkte zu klären:

- Definition von Standards für Serviceprovider:
  Als weitere Schritte wären sogenannte Eignungskriterien für Cloud-Service-Provider zu entwickeln (Beispiel aus dem Bundesbereich: Klassifizierung von Inhalten nach Sicherheitsklassen ergänzen bzw. überarbeiten und die Eignung für ein gewisses Cloudmodell anführen; z.B. RIS geeignet für Public Cloud)
- Sicherstellen der Nachhaltigkeit:
  Anwendungen und Services die in Form von Cloud Services ausgelagert werden, müssen unabhängig vom Cloud Modell (Private Cloud, Public Cloud, Hybrid Cloud) den zeitlich und organisatorischen Übergang zu einem anderen Service Provider (oder Inhouse) in einem vorgegebenen Rahmen sicherstellen.
- Wirtschaftlichkeits-Beurteilung:
  Entsprechende ROI Kriterien für die Einführung von Cloud Services wären gemeinsam festzulegen (z.B. ROI innerhalb von 2,5 Jahren einbringbar/ garantiert wird, Haftung am ROI an Umsetzer überbindbar ist, …).
- Nutzen aus Cloudeffekten ermöglichen / Cloud Informationspolitik:
  Als Grundlage zur Entscheidung ob der Betrieb eines IT-Services in der Cloud oder klassisch in einem Rechenzentrum erfolgt, ist zu definieren, was unter "Cloud-fähig" zu verstehen ist, bzw. welche Charakteristika Voraussetzungen für einen Betrieb in einer Cloud erforderlich sind.
- Cloud Charakterisitika:
  - **Anforderungen an Cloud-Applikationen** *TopDown: WAS muss ich tun, um Cloud-fähig zu werden/etwas in die Cloud integrieren zu können* wenn eine Applikation, ein Services, etc. neu oder angepasst bereitgestellt wird.
  - **Anforderungen an Cloud-Nutzer** Welche Voraussetzungen müssen erfüllt sein, dass eine Nutzung von Diensten aus der Cloud erfoglreich ist und entsprechende Nutzen bringt.
  - **Ermöglichen von QuickWins** *Was ist jetzt bereits ohne großen Aufwand möglich?*