CHECKLISTE SICHERE PASSWÖRTER

Sichere Auswahl und Handhabung von Passwörtern
Für Behörden, Institutionen, Unternehmen und auch Privatanwender/innen

ID	AKTIVITÄT	STATUS	
I	**PASSWORT-FESTLEGUNG**		
01	Auswählen starker und zufälliger Passwörter die schwer zu erraten sind.	OK	KO
02	Das Passwort sollte trotz Komplexität gut merkbar sein.	OK	KO
03	Im Idealfall Passwörter mittels geeigneter Hilfsprogramme automatisch generieren.	OK	KO
04	Das Passwort soll Großbuchstaben enthalten.	OK	KO
05	Das Passwort soll Kleinbuchstaben enthalten.	OK	KO
06	Das Passwort soll Ziffern enthalten.	OK	KO
07	Das Passwort soll Sonderzeichen enthalten.	OK	KO
08	Die Passwortlänge sollte dem Einsatzzweck angemessen sein, also mindestens neun Zeichen für Online-Dienste und entsprechend mehr für sensible Online-Dienste (z.B. solche mit personenbezogenen oder finanziellen Daten, Cloud-Dienste) und Offline-Anwendungen/-Verschlüsselung.	OK	KO
09	Keine Standard-Passwörter oder gängige Muster bzw. leicht zu erratende Wörter verwenden (z.B. 123456, passwort, qwertz, asdfgh, admin).	OK	KO
10	Kein triviales Passwort mit einer simplen Ergänzung verwenden, z.B. durch Anhängen eines Rufzeichens oder Ziffern.	OK	KO
11	Keine persönlichen Details verwenden, die Dritten bekannt sein können (z.B. Name, Geburtsdatum, Adresse, Name des Haustiers); auch nicht als Teil des Passworts.	OK	KO
12	Keine Wörter verwenden die auch in einem Wörterbuch vorkommen, auch nicht mehrfach hintereinander.	OK	KO
13	Keine direkten Referenzen oder Bezeichnungen für den jeweiligen Dienst im Passwort verwenden.	OK	KO
14	Falls das Passwort möglicherweise auch auf anderssprachigen Tastaturen eingegeben werden muss, sollte bei der Passwortauswahl auf darauf fehlende Umlaute und Sonderzeichen verzichtet werden. Es ist zu berücksichtigen, dass Sonderzeichen dabei eventuell auf andere Tasten kodiert sind.	OK	KO
15	Keine einem einheitlichen Muster folgenden Passwörter verwenden, durch die bei Kenntnis eines Passworts auf weitere Passwörter geschlossen werden kann.	OK	KO
II	**PASSWORT-VERWENDUNG**		
16	Passwort geheim halten und mit niemandem teilen.	OK	KO
17	Passwort nur unbeobachtet eingeben. Gegebenenfalls die Anzeige der eingegebenen Passwort-Zeichen im Browser deaktivieren.	OK	KO
18	Passwort nur auf vertrauenswürdigen Geräten eingeben. Auch sollten Passwörter nur über vertrauenswürdige Netzwerke (z.B. eigenes, gesichertes WLAN) eingegeben werden.	OK	KO
19	Passwort nur für die jeweils vorgesehene Anwendung (z.B.: zuverlässige Webseite, Applikation) eingeben.	OK	KO
20	Dasselbe Passwort nur für einen Anwendungsfall bzw. Dienst verwenden.	OK	KO
21	Sperren von Computern bzw. anderen Geräten mit Benutzerkonten oder abschalten, wenn diese nicht genützt werden.	OK	KO
22	Abmelden von Webseiten wenn man diese verlässt (das Schließen der Webseite reicht nicht aus).	OK	KO
23	Voreingestellte (Default-)Passwörter vor Inbetriebnahme bzw. Verwendung ändern.	OK	KO
24	Keine Passwörter teilen bzw. versenden, insbesondere nicht über ungesicherte Kanäle (wie z.B.: E-Mail, Fax, Internet, Messenger-Dienste). Auch nicht bei einer Aufforderung.	OK	KO

III	PASSWORT-MANAGEMENT		
25	Passwort-Manager zur Verwaltung der Passwörter und Zugangsdaten verwenden.	OK	KO
26	Definieren starker Master-Passwörter für den Zugriff auf den Passwort-Manager	OK	KO
27	Passwort zeitnah ändern bei Kompromittierung oder Verdacht einer Kompromittierung eines Passworts (z.B.: unberechtigte Verwendung).	OK	KO
28	Passwörter nicht im Browser speichern. Ist das nicht vermeidbar, sind diese zumindest durch ein starkes Master-Passwort zu schützen.	OK	KO
29	Keinesfalls auf fremden Geräten Passwort-Dateien und darin hinterlegte Passwörter speichern.	OK	KO
30	Passwörter nicht im Klartext aufschreiben und aufheben, insbesondere nicht als Notiz auf dem Monitor oder der Schreibtischauflage. Wenn eine Erinnerung trotzdem notwendig ist, dann nur in geschützter Form, sodass niemand sonst davon weiß und darauf zugreifen kann.	OK	KO
31	Passwort-Dateien nicht mit Dritten teilen bzw. austauschen.	OK	KO
32	Änderung von Passwörtern ausschließlich durch Zeitablauf (z.B.: 1x pro Quartal) ist nicht mehr zeitgemäß.	OK	KO
IV	**HÄRTUNGSMASSNAHMEN**		
33	Einen zweiten unabhängigen Authentifizierungsfaktor (z.B. Besitz, Wissen, Biometrie) für den Passwort-Manager-Zugang und dort wo Passwörter verwendet werden – sofern eine solche Einstellung verfügbar ist – aktivieren.	OK	KO
34	Zusätzliche Verschlüsselung der Passwort-Manager-Datenbank, beispielweise durch Speicherung in einem verschlüsselten Container.	OK	KO
35	Aktivieren einer automatischen Abmeldung (z.B. Webseiten) bzw. Sperrung (z.B. Betriebssystem) nach einer bestimmten Zeitspanne, sofern eine solche Einstellung verfügbar ist.	OK	KO
V	**RICHTLINIEN UND ANLASSBEZOGENE MASSNAHMEN**		
36	Bei Befall mit Schadsoftware oder wenn davon ausgegangen werden kann, dass ein Passwort kompromittiert wurde, nach der Bereinigung alle Passwörter ändern die betroffen sein könnten.	OK	KO
37	Im Unternehmensumfeld oder bei größeren Organisationen sollte – sofern für den jeweiligen Anwendungsfall möglich und notwendig – ein Master-Passwort für unvorhergesehene Ausfälle oder bei Personalwechsel eingesetzt werden.	OK	KO
38	Auswählen und festlegen zumindest einer Sicherheitsfrage, deren Antwort schwer zu erraten ist, um beispielsweise ein vergessenes Passwort wiederherzustellen. Frage und Antwort sind so zu wählen, dass niemand anders diese beantworten kann. (Wichtig: Zuerst Abwägen ob notwendig, da bei schlechter Auswahl der Frage diese auch als Einfallstor für die Kontoübernahme dienen kann!)	OK	KO