Richtlinie zur Regelung des Passwortgebrauches für Benutzer

Version: ###Version###

Status: ###Status###

Dokumenteninformationen

Richtlinie zur Regelung des Passwortgebrauches für Benutzer	
###Name der Organisation###	
Version	###Version###
Status	###Entwurf | Review | Freigabe | Ungültig###
Datum der letzten Änderung	###Datum###
Verantwortung	###Name des Verantwortlichen###
Klassifizierung	###S1 öffentlich | S2 intern | S3 geheim###
Gültigkeitszeit	###Zeitraum###
Überarbeitungsintervall	###Anzahl Jahre### Jahre
Nächste Überarbeitung	###Monat Jahr###
Dateiname	###Dateiname###
Ablageort	###Ablageort###

Änderungsübersicht

Lfd. Nr.	Datum	Version	Änderungen	Durchgeführt von
1				
2				
3				
4				
5				
6				
7				

Inhalt

1 Veranlassung, Gegenstand der Richtlinie

Elektronische Daten dürfen nur von berechtigten Personen gelesen oder bearbeitet werden. Deshalb müssen sich diese Personen mittels individueller Zugangsdaten vor Beginn der Verarbeitung am verarbeitenden System authentisieren.

Dazu teilen sich die Person und das System zuvor vereinbarte geheime Informationen. Im Zuge der Anmeldung übermittelt die Person die geheimen Informationen auf einem sicheren Weg an das System. Dieses vergleicht die Übermittlung mit dem im System hinterlegten Werten und gibt im Erfolgsfall den Zugriff frei.

Die geheimen Informationen bestehen in der Regel aus einem oder mehreren Passwörtern. Um diese geheim zu halten, dürfen sie nicht leicht zu erraten sein und müssen sicher verwahrt werden.

Diese Richtlinie regelt den Passwortgebrauch für Beschäftigte in ###Name der Organisation###. Die Richtlinie dient damit der Erfüllung der relevanten Anforderungen der Basisabsicherung nach der BSI-Grundschutzmethodik (Baustein ORP.4 Identitäts- und Berechtigungsmanagement, Anforderungen 8 und 22) und ist ein Beitrag, um die „Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“ (vgl. Art. 32 DSGVO).

2 Regelungen

2.1 Regelung des Passwortgebrauchs

Die folgenden Regelungen gelten für alle Beschäftigten der ###Name der Organisation###:

1. Passwörter dürfen nicht mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden.
2. Passwörter müssen geheim gehalten werden. Sie dürfen nur dem Benutzer persönlich bekannt sein und nur verschlüsselt übertragen werden. Bei Online-Diensten ist eine verschlüsselte Übertragung gegeben, wenn die Adresse (URL) mit „https://“ beginnt und das zugrunde liegende Zertifikat des Dienstanbieters von einer vertrauenswürdigen Stelle ausgestellt wurde. Werden Passwörter innerhalb von Dateien übertragen, so müssen diese vorher mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt werden (z.B. AES-256 implementiert z.B. in den Anwendungen VeraCrypt und 7-Zip).
3. Passwörter dürfen nur unbeobachtet eingegeben werden.
4. Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.
5. Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
6. Voreingestellte Passwörter müssen sofort nach der ersten Anmeldung geändert werden.
7. Für Sicherheitsfragen zur Wiederherstellung von Passwörtern sollten keine realen Sachverhalte verwendet werden. Es sollten willkürliche Fragen und Antworten verwendet und sicher fixiert werden.
8. Passwörter dürfen für einen Notfall schriftlich oder elektronisch hinterlegt werden. Bei einer Vielzahl von komplexen Passworten dürfen sie auch hinterlegt werden, um sie sich in Erinnerung zu rufen.

9. Hinterlegte Passwörter müssen sicher aufbewahrt werden. Schriftlich hinterlegte Passwörter müssen in abgeschlossenen Räumen und Schränken aufbewahrt werden, zu denen nur Berechtigte Zugang haben.
10. Elektronisch gespeicherte Passwörter dürfen nicht in Cloud-Speichern abgelegt werden. Sie müssen mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt werden (z.B. AES-256 implementiert z.B. in den Anwendungen VeraCrypt und 7-Zip).
11. In Web-Browsern integrierte Passwortmanager dürfen nicht verwendet werden.

2.2 Regelung zur Passwortqualität

In Abhängigkeit von Einsatzzweck und Schutzbedarf müssen Passwörter geeigneter Qualität gewählt werden. Ist mit dem damit verbundenen Zugang nicht nur lesender sondern auch schreibender Zugriff möglich, ist eine höhere Qualität erforderlich. Der Schutzbedarf bemisst sich nach dem Grad der Vertraulichkeit der zugänglichen Informationen. Bei personenbezogenen Daten und geheimen Informationen ist der Schutzbedarf sehr hoch.

Passwörter gelten als sehr sicher, wenn sie aus einer Kombination von mindestens 12 Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+…) bestehen. Länderspezifische Sonderzeichen (wie z. B. Umlaute ä, ö, ü, Ä, Ö, Ü und ß) sollten nicht verwendet werden.

Triviale Passwörter, z.B. bestehend aus Namen, Wörtern aus Wörterbüchern, Tastaturfolgen oder gängigen Beispielen dürfen nicht verwendet werden.

3 Empfehlungen

3.1 Einsatz eines Passwortmanagers

Mit zunehmender Anzahl von Authentisierungsdaten erhöht sich für Benutzer die Schwierigkeit, diese sicher aufzubewahren und doch unkompliziert abzurufen.
In diesem Fall empfiehlt sich die Speicherung der Authentisierungsdaten in einem geeigneten Passwortmanager. Der Benutzer benötigt damit zur Anmeldung an verschiedene Systeme nur noch diese Anwendung und die Authentisierungsdaten dafür („Masterpasswort“).
Der Schutzbedarf für diese Anwendung ist sehr hoch. Das Masterpasswort ist durch den Benutzer sehr komplex zu gestalten.

Ein geeigneter Passwortmanager muss dabei mindestens folgende Funktionalitäten zur Verfügung stellen:

- Die Authentisierungsdaten müssen mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt gespeichert werden.
- Nach einem vorgegebenen Inaktivitäts-Zeitraum oder der Aktivierung der Bildschirmsperre sollte der Passwortmanager den Zugriff sperren.
- Der Passwortmanager muss eigenständig prüfen, ob Updates verfügbar sind.
- Authentisierungsdaten sollten sich gruppieren lassen.
- Es sollten Web-Browser-Erweiterungen zur automatisierten Befüllung der Anmeldeformularfelder zur Verfügung stehen.
- Bei der Änderung von Authentisierungsdaten sollten die bisherigen nicht gelöscht, sondern als vorherige Version gespeichert werden.
- Zeitbasierte Einmalkennwörter (Time based One Time Password - TOTP) entsprechend dem Standard RFC-6238[1] sollten generiert werden können (Einschränkung s.u.).

Die Datei, in welcher die Authentisierungsdaten verschlüsselt gespeichert sind, darf nur auf Speichermedien und Laufwerken gespeichert werden, welche nur dem Eigentümer zugänglich sind. Die Datei darf nicht bei einem Cloud-Dienst gespeichert werden, welcher außerhalb des Geltungsbereiches der Datenschutz-Grundverordnung (DSGVO) liegt.
Kommt ein Angreifer in den Besitz dieser Datei, könnte er versuchen, diese zu entschlüsseln (z. B. mittels Brute-Force-Methode[2]).

Es sollten regelmäßig Backups dieser Datei oder eines Exports der im Passwortmanager gespeicherten Daten angefertigt werden. Eine Exportdatei muss verschlüsselt abgelegt werden.

Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, müssen diese Funktionen und Plug-ins deaktiviert werden.
Die Aktivierung einer Anwendung zum Viren- und Bedrohungsschutz auf dem Client-PC, auf welchem der Passwortmanager arbeitet, ist obligatorisch.

###eventuell Empfehlung eines konkreten Produktes###

[1] Standard RFC-6238
https://de.wikipedia.org/wiki/Time-based_One-time_Password_Algorithmus

[2] Brute-Force-Methode
https://de.wikipedia.org/wiki/Brute-Force-Methode

3.2 Zwei-Faktor-Authentifizierung

Kommen Unberechtigte in den Besitz von Passwörtern, besteht die Gefahr, dass diese anstelle des Eigentümers Daten lesen und bearbeiten können.

Einen zusätzlichen Schutz bietet hier die Übermittlung eines zweiten Authentisierungsfaktors. Wenn die datenverarbeitenden Systeme ein solches Verfahren anbieten, sollte es genutzt werden.

Die verwendeten Faktoren sollten aus den unterschiedlichen Kategorien

- Besitz (z. B. Chipkarte, TAN-Generator, Smartphone-App als TOTP-Generator),
- Wissen (z. B. PIN) und
- biometrische Merkmale (z. B. Fingerabdruck)

stammen.

Bei der mittelbaren Zwei-Faktor-Authentifizierung besteht der „Besitz“ oft aus einer App auf dem Smartphone, welche das Geheimnis speichert. Der Schutzbedarf für diese App ist sehr hoch. Zum Öffnen ist ein komplexes Passwort anzuwenden.
Die Daten auf dem Smartphone sollten verschlüsselt sein.

Werden mit einem Passwortmanager Passwörter und zeitbasierte Einmalkennwörter verwaltet, stammen die Faktoren genau genommen nicht mehr aus unterschiedlichen Kategorien. Trotzdem ist damit die Sicherheit, gegenüber der ausschließlichen Verwendung eines Passwortes, erhöht.

Bei der Übermittlung von Einmalkennwörtern per SMS sollte das Empfangsgerät ein anderes sein, als jenes, mit welchem das Datenverarbeitungssystem bedient wird.

4 Inkrafttreten

Diese Richtlinie zur Regelung des Passwortgebrauchs in ###Name der Organisation### tritt mit Unterzeichnung in Kraft und setzt vorhergehende Versionen außer Kraft.

###Ort###, den ###Datum###

###Unterschrift###

###Funktionsbezeichnung des Unterzeichnenden###