Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Umgang mit Passwörtern

Ratgeber zum Datenschutz

Umgang mit Passwörtern

Ratgeber zum Datenschutz

Herausgeberin:

Berliner Beauftragte für
Datenschutz und Informationsfreiheit

Friedrichstr. 219
Besuchereingang: Puttkamerstr. 16-18
10969 Berlin
Telefon: 030 13889-0
Telefax: 030 2155050
E-Mail: mailbox@datenschutz-berlin.de

Gestaltung: april agentur GbR
Druck: ARNOLD group.

Stand: Juni 2020

Einleitung

Um die Vertraulichkeit, Integrität und Authentizität personenbezogener Daten bei der Nutzung von (Online-) Diensten gewährleisten zu können, muss die Identität der Nutzenden überprüft werden. Diese Identifizierung und Authentifizierung geschieht in der Regel durch die Eingabe einer Kombination aus persönlicher Kennung (Benutzername) und geheimem Passwort. Wer Kennung und Passwort kennt, kann sich authentifizieren.

Bei Verfahren mit normalem Schutzbedarf kann eine solche Authentifizierung derzeit gerade noch als hinreichend angesehen werden. Von normalem Schutzbedarf ist dann auszugehen, wenn weder große Datenmengen noch sensible oder sensitive Daten verarbeitet werden. Um sensitive Daten handelt es sich, wenn sie nach der Datenschutz-Grundverordnung zu besonderen Kategorien mit erhöhtem Schutzbedarf zählen, also etwa Gesundheitsdaten oder Daten über Herkunft, Religion oder sexuelle Orientierung der Betroffenen.

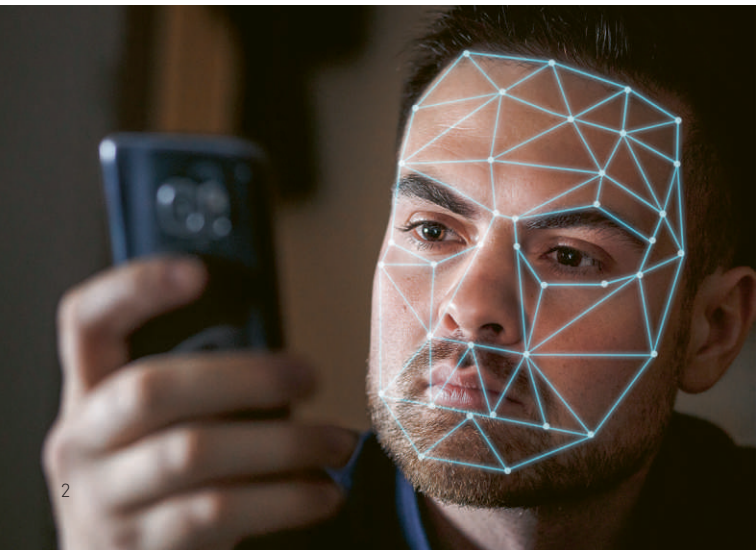
Sobald Anwendungen und Dienste Zugriff auf sensible, sensitive oder eine große Anzahl von personenbezogenen Daten ermöglichen, besteht ein erhöhter Schutzbedarf, der eine stärkere Absicherung der Daten mit einem oder mehreren weiteren Faktoren erforderlich macht. Möglichkeiten für eine solche Mehrfaktor-Authentifizierung sind z. B.:

- **Abfragen über den Besitz physischer Geräte, die mit dem Dienst verknüpft sind (Hardware-Token, der zeitabhängig eine TAN ausgibt oder über den USB-Port mit dem Dienst kommuniziert, Chipkarte, SMS-TAN, mTAN) oder**

- **Abgleich von biometrischen Daten (also von Körpermerkmalen, etwa durch einen Iris-Scan, Fingerabdruck oder Gesichtserkennung).**

Bei der Verwendung von biometrischen Daten zur Authentifizierung ist jedoch zu beachten, dass diese selbst zu den besonderen Kategorien personenbezogener Daten gehören und daher besonders schutzbedürftig sind.

Unabhängig von Art und Umfang der verarbeiteten Daten sollte, wo immer möglich, eine Mehrfaktor-Authentifizierung genutzt und aktiviert werden.



Passwortmanager und Single-Sign-On-Dienste

Menschen nutzen immer mehr Online-Dienste und müssen sich heute eine Vielzahl von Kennungen und Passwörtern merken. Bei der Menge an pro Person genutzten Konten wird es für die Nutzenden immer schwieriger, sich alle Zugangsdaten zu merken. Häufig führt dies dazu, dass für mehrere Dienste dasselbe Passwort verwendet wird. Dies ist jedoch äußerst riskant, da Unbefugte bei Kenntnis eines Passworts eventuell Zugang zu einer Vielzahl von Diensten erreichen können.

Der Einsatz eines Passwortmanagers kann hier eine Lösung sein. Ein Passwortmanager ist ein Programm, das lokal die verschiedenen Zugangsdaten einer Person zumindest mit einem sogenannten Masterpasswort verschlüsselt speichert.

Folgende Kriterien sollten bei der Auswahl und Nutzung eines Passwortmanagers berücksichtigt werden:

- **Das für die Anmeldung beim Passwortmanager erforderliche Masterpasswort sollte besonders sicher sein.**

- **Der Passwortmanager sollte über eine verschlüsselte Speicherung mit einem anerkannten Kryptographie-Verfahren verfügen, also die Daten sicher verschlüsseln. Bekannte Verfahren sind z. B. 3DES (Data Encryption Standard) oder AES (Advanced Encryption Standard).**

- **Zumindest bei der Verarbeitung sensibler und sensitiver Daten sollten die im Passwortmanager gespeicherten Zugangsdaten nicht in einer Cloud hinterlegt werden.**

Zur Vermeidung einer Vielzahl von Zugangsdaten können auch sogenannte „Single-Sign-On-Dienste“ als Alternative zum Passwortmanager genutzt werden. Hierbei handelt es sich um Angebote zur Einmal-Anmeldung, also um Dienste, die es Nutzerinnen und Nutzern erlauben, nach nur einmaliger Authentifizierung direkt auf verschiedene Dienste, für die sie berechtigt sind, zuzugreifen. Hierfür gibt es einige Anbieter wie z. B. Verimi, NetID, Facebook oder Google.

Allerdings haben Single-Sign-On-Dienste entscheidende Nachteile, weswegen der Einsatz nur bedingt empfohlen werden kann:

- **Der Single-Sign-On-Dienst erhält Nutzungsdaten über die zugänglich gemachten Dienste.**

- **Falls ein Single-Sign-On-Dienst erfolgreich gehackt wird, hat der Angreifer Zugriff auf viele Nutzungskonten (auch bei den Drittdiensten), für die der Single-Sign-On-Dienst verwendet wurde.**

Deshalb ist bei der Nutzung von Single-Sign-On-Diensten besonders zu beachten:

- **Das Passwort zum Single-Sign-On-Dienst sollte besonders sicher sein. Eine Zwei-Faktor-Authentifizierung sollte angeboten und aktiviert werden.**

- **Da der Single-Sign-On-Dienst grundsätzlich Zugriff auf alle Nutzungskonten hat, für die er verwendet wird, ist die Wahl eines besonders vertrauenswürdigen Anbieters entscheidend.**

Grundsätzliches

Erfolgt die Authentifizierung einer Person allein durch die Abfrage von Wissen, also über Kennung und Passwort, sollte Folgendes beachtet werden:

- **Das Passwort sollte geheim gehalten und nicht an andere Personen weitergegeben werden.**
- **Wird ein Passwort unautorisierten Personen bekannt, so ist es unverzüglich zu ändern.**
- **Bei der Eingabe des Passwortes sollte darauf geachtet werden, dass keine unbefugten Personen die Eingabe beobachten können.**

Anforderungen an ein sicheres Passwort

- Je länger ein Passwort ist, desto besser ist der Schutz. Die absolute Mindestlänge von Passwörtern sollte acht Zeichen betragen.

- Es sollten Passphrasen, d. h. lange Wortfolgen genutzt werden. Passphrasen könnten beispielsweise wie folgt gebildet werden:

+ „Meinen 1. Urlaub an der Ostsee habe ich bei viel Sonnenschein ueberwiegend im kuehlen Nass beim Sammeln von 847 Muscheln verbracht." Oder gekürzt auf jeweiligen ersten Buchstaben der einzelnen Wörter eines Satzes ohne Leerzeichen: „M1.UadOhibvSuikNbSv847Mv."

+ „Jeden 1. Mittwoch im Monat sind 2 lila Umlaufmappen, mit Namenskuerzel gekennzeichnet, in das Posteingangsfach des Abteilungsleiters zu legen!" Gekürzt auf den jeweiligen ersten Buchstaben der einzelnen Wörter ohne Leerzeichen wird daraus: „J1.MiMs2lU,mNg,idPdAzl!"

- Durch die Verlängerung des Passwortes lassen sich die Kombinationsmöglichkeiten bei der Zeichenauswahl erhöhen und so die Erfolgsaussichten von „Hackern“ senken.

- Das Passwort kann auch aus einem alphanumerischen Zeichenmix mit Sonderzeichen gebildet werden. Je individueller, desto besser.

- Das Passwort sollte in keinem Wörterbuch stehen, denn diese werden standardmäßig bei Angriffen zu Hilfe genommen.

- Beliebte Tastenkombinationen wie 12345678, qwert, password, 1q2w3e o. Ä. sind zu vermeiden.

- Ebenfalls zu vermeiden sind sogenannte Trivialpasswörter, die sich aus Namen, Geburtsdaten oder Kfz-Kennzeichen herleiten lassen.

- Außer für Anwendungen mit höherem Schutzbedarf sollte ein zwangsweiser zyklischer Wechsel des Passworts nicht erzwungen werden. Dafür ist aber ein ausreichend langes sicheres Passwort zu bilden.

- Die Wiederverwendung eines bereits benutzten Passworts sollte erst nach mindestens fünf Wechseln erfolgen.

- Vorgegebene Start- bzw. Initial-Passwörter eines Dienstes sollten immer unverzüglich geändert werden, da diese mit hoher Wahrscheinlichkeit Dritten bereits bekannt und auch leicht zu erraten sind.

Hilfen

- Mit dem Webdienst „Pwnd Password“ kann überprüft werden, ob sich Ihr Passwort auf einer Liste von gehackten Passwörtern befindet.

- Von der Zeitschrift c’t werden unter anderen folgende Passwortmanager mit guten bis sehr guten Bewertungen ausgezeichnet:

  + Bitwarden von 8bit Solutions LLC
  + Dashlane von Dashlane
  + Enpass von Sinew Software Systems
  + LasPass von LogMeIn
  + SafeInCloud von Andrey Shcherbakov

Mehr Informationen im Internet
www.datenschutz-berlin.de
www.datenschutz.de

www.datenschutz-berlin.de