audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Passwortsicherheit und Passwortmanager

Zusammenfassung

Die einfachste und häufigste Möglichkeit um IT-Systeme und Informationen vor unbefugtem Zugriff zu schützen sind Passwörter. Fast jede Webanwendung, aber auch viele interne Systeme sind mit Passwörtern geschützt und sollen die Vertraulichkeit der gespeicherten Daten gewährleisten. Also nur den berechtigten Personen den Zugriff ermöglichen. Doch Passwörter haben auch viele Schwachstellen: sie können ausgespäht, unsicher gespeichert oder übertragen, erraten oder geknackt werden. Sowohl im beruflichen wie auch privaten Umfeld sollte der Passwortsicherheit daher ein besonderer Stellenwert zukommen.

Laut einer Studie des Onlinedienstes web.de nutzen 59% der Befragten ihre Passwörter mehrfach in verschiedenen Diensten. Das Hauptproblem hierbei ist, wird ein Dienst gehackt, können die gestohlenen Passwörter meist in Kombination mit der gestohlenen E-Mail-Adresse auch zum Zugriff auf andere Inhalte genutzt werden. Daher sollten bestimmte Sicherheitsstandards für Passwörter eingefordert und eingehalten werden.

Problemstellung

Passwörter sollen möglichst lang und komplex sein und dabei jeweils nur für einen Einsatzzweck verwendet werden. Das überfordert jedoch so ziemlich alle Benutzer und führt zu Haftnotizen unter Tastatur mit den wichtigsten Kennwörtern, zu Passwortlisten in Excel oder anderen einfallsreichen Ideen, um das Passwort-Chaos möglichst „benutzerfreundlich“ aber nicht sicher zu gestalten. Auch die in modernen Webbrowsern eingebauten Passwortspeicher sind nur bedingt geeignet, da deren Nutzung meist keine weitere Hürde verlangt, als den Browser öffnen zu können. Damit ist ein nicht gesperrter Arbeitsplatz PC oder ein gestohlener Laptop eine leichte Beute für einen Passwortmissbrauch. Weiterhin muss man bedenken, dass wir heute Anwendungen über das Internet auch gerne auf dem Smartphone benutzen möchten und somit die Verteilung der Passwörter ebenfalls eine wichtige Rolle spielt.

Daher gilt unsere Hilfestellung den verschiedenen Anforderungen der Passwortsicherheit und der praxisnahen Umsetzung.

Anforderungen an sichere Passwörter

Die höchste Sicherheit bei der Authentifizierung bilden eine Kombination aus Passwörtern (Wissen) und Besitz (z. B. Zugriff auf ein Token oder eine Smartphone-App) welche man als MFA (Multi-Faktor-Authentifizierung) bezeichnet. Da MFA aber nicht überall implementiert ist, bleibt es häufig beim Passwort als alleinigem Sicherheitsmerkmal und für dieses müssen einige Punkte bedacht werden, damit eine Mindestsicherheit gewährleistet werden kann.

Die wichtigsten Anforderungen an sichere Passwörter lässt sich in den folgenden 5 Punkten zusammenfassen:

1. **Lange Passwörter:** Verwenden Sie möglichst 12 Zeichen oder mehr, denn umso länger das Passwort, umso schwerer ist ein Angriff auf dieses.
2. **Komplexe Passwörter:** Verwenden Sie möglichst alle Zeichen, die Ihnen die Tastatur bietet (Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen) in möglichst zufälligen Kombinationen.
3. **Ein Passwort pro Dienst:** Passwörter sollen nicht mehrfach verwendet werden. Ist ein Dienst (z. B. Webanwendung) und das darin verwendete Passwort gehackt, sind die anderen Passwörter davon meist nicht betroffen.
4. **Seltenes Passwortwechseln:** Wechseln Sie Ihr Passwort nicht zu häufig, denn ansonsten vergibt man gerne Reihenfolgen wie „Passwort1“, „Passwort2“, um sich das Merken zu vereinfachen.

5. **Passwortmanager nutzen:** Auch wenn es viele Möglichkeiten zum Passwortmerken gibt, irgendwann stößt jede noch so gute Eselsbrücke oder Passwortkarte an ihre Grenzen und ein professioneller Passwortmanager schafft Abhilfe.

Anforderungen an Passwortmanager

Mit Hilfe spezieller Software (sog. Passwortmanager) lässt sich die Verwaltung der unzähligen Passwörter sehr gut handhaben. Dazu kann man zwischen lokaler Software und webbasierten Diensten wählen. Wobei sich gerade bei den Webdiensten ein gewisser Vertrauensvorschuss für die Betreiber und deren Sicherheitskonzept als Voraussetzung aufdrängt. Wer das Ganze lieber möglichst in seiner eigenen Obhut belassen möchte, kann eine lokale Software nutzen, welche die sicher verschlüsselten Daten über Cloudspeicher auf andere Geräte synchronisieren und damit auch eine Ausfallsicherheit gewährleisten kann.

Die folgenden Anforderungen sollten sowohl bei einem lokalen, als auch einem cloudbasierten Passwortmanager beachtet werden:

1. **Zwei Faktoren für Zugriff:** Der Login zum Passwortmanager sollte mit 2 Faktoren geschützt werden, damit die hochsensiblen Daten nicht durch einen einfachen Passwortdiebstahl entwendet werden können.
2. **Ende-zu-Ende Verschlüsselung:** Der Datenspeicher in welchem die Passwörter abgelegt werden muss unbedingt komplett verschlüsselt sein. Mindestens mit einem AES256 Verfahren. Die reine Übertragungsverschlüsselung im Internet SSL/TLS reicht hier nicht aus.
3. **Zwischenablage reinigen:** Passwörter werden für den Bedienkomfort gerne in die Zwischenablage des Computers kopiert. Dort sollten Sie nach einer kurzen Zeitspanne wieder automatisch entfernt werden.
4. **Abmelden bzw. Sperren:** Wenn Sie das Endgerät (PC, Smartphone, etc.) nicht benutzen sollten Sie den Passwortmanager sperren oder sich abmelden.
5. **Open-Source oder vertrauenswürdige Hersteller:** Gibt es einen Passwortmanager in einer Open-Source-Variante kann man sich den Quellcode anschauen und dort Sicherheitsanalysen durchführen. Solche Dienste bieten den Vorteil, dass Hintertüren oder Sicherheitsprobleme schneller von Experten erkannt und veröffentlicht werden können. Ebenfalls gute Erfahrungen können mit vertrauenswürdigen Herstellern von Sicherheitssoftware gemacht werden, die auch entsprechend in die Sicherheitstechnik investieren. Allerdings bleibt hier immer ein Restrisiko des Hintertürchens bestehen.

In folgende Liste finden Sie einige bekannte Passwortmanager und unsere Sicherheitsbewertung:

https://www.audatis.de/aktuelles/passwortmanager

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

LinkedIn | Twitter | XING

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Auswahl von datenschutzkonformen und sicheren Passwortmanagern und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung des Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de