Das Schweizer Industriemagazin. Seit 1972. www.maschinenbau-schweiz.ch

maschinenbau

Nr. 7 Juli 2023

Bild: Pixabay

Passworte dürfen keine persönlichen Daten enthalten.

Das Passwort ist tot, lang lebe das Passwort

Jeden Monat werden tausende von Kennwörtern bei Hacker-Angriffen gestohlen. Zudem verwenden immer noch viele Menschen schlechte Kennwörter. Das Beliebteste ist noch immer 123456, gefolgt von password oder hallo. Wenn das gleiche Kennwort noch für diverse Zugänge genutzt wird, wird es gefährlich. Doch es gibt inzwischen Alternativen.
Die Top 200 Passwörter können unter https://nordpass.com/most-common-passwords-list/ abgerufen werden.

Dass Passwörter unsicher sind, ist schon lange bekannt. Viele Firmen definieren daher Vorgaben an Kennwörter. Dies könnten beispielsweise sein:

- Länge von mindestens zwölf Zeichen
- Benutzung mindestens einer Ziffer
- enthält mindestens ein Sonderzeichen
- enthält mindestens einen Grossbuchstaben und einen Kleinbuchstaben
- das Passwort darf nicht in einem Wörterbuch enthalten sein, darf kein Wort im Dialekt oder in der Umgangssprache irgendeiner Sprache oder irgendein solches Wort rückwärts geschrieben sein.
- Passworte dürfen keine persönlichen Daten enthalten (zum Beispiel Geburtsdatum, Adresse, Name von Familienmitgliedern, usw.)

Idealerweise wird ein Satz gebildet und jeweils das erste Zeichen davon benutzen. Aus «Heute ist ein wunderschöner Tag zum etwas Neues zu lernen!» wird «Hi1wsTzeNzl!».

ZUM AUTOR

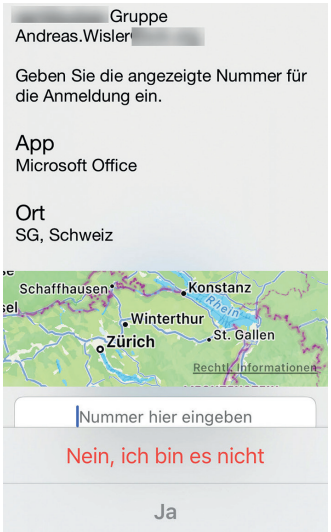
Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Passwort testen

Der Datenschutzbeauftrage des Kantons Zürich hat eine Seite ins Internet gestellt, mit welcher die Qualität des eigenen Passworts getestet werden kann. Sie finden diese unter www.passwortcheck.ch. Folgende Beispiele zeigen, welche Zeit benötigt wird, um ein Passwort zu knacken:

- Good: <1 s
- NuLh@z%7: 15 min
- GoodOldTimes: 16 min
- G00d0ldTime$: 11 Tage
- G%%d%ldTime$: 17 Jahre
- GoodOldTimesComeBack: 3 Jahre
- GoodOldT!mesC0meBack: 305 Jahre
- wUqw9CriS3@NutLh@z%7: >1 Mio Jahre



Beispiel einer Push-Nachricht, mit Nummer-Eingabe.

Viele Webseiten verlangen heute zusätzlich einen weiteren Faktor. Daher wird von 2-Factor- (2FA) oder Multifactor Authentication (MFA) gesprochen. Bekannt sind unter anderem Google Authenticator oder der Microsoft Authenticator. Zweiterer hat den Vorteil, dass eine Push-Nachricht geschickt wird und diese muss bestätigt werden. Hacker haben versucht, auch dies zu überlisten, indem sie so viele Push-Nachrichten schicken, bis der Benutzer entnervt eine anklickt. Daher hat Microsoft Mitte Mai damit begonnen, nicht nur einen Klick zu akzeptieren, sondern es muss die angezeigte Zahl ebenfalls eingegeben werden. Dies ist zwar mühsam, erhöht die Sicherheit aber massiv.

Nie Passworte aufschreiben

Weitere allgemeine Regeln, die für Kennwörter eingehalten werden sollen:

- Niemals Passworte im Browser für automatisches Login speichern
- Unterschiedliche Passwörter für jede Applikation verwenden
- Nie Passworte aufschreiben (ausser wenn diese sicher verwahrt werden)
- Passworte, die für private Zwecke genutzt werden, dürfen nicht für Geschäftszwecke benutzt werden (und umgekehrt)
- Niemals Passworte per E-Mail verschicken. Dazu sollte besser SMS oder einen Ende-zu-Ende verschlüsselter Messaging Service wie Threema, Signal oder WhatsApp verwendet werden
- Ein Passwort muss sofort geändert werden, sobald der Verdacht da ist, dass es kompromittiert worden ist

Um zu wissen, ob ein Passwort bereits gestohlen wurde, lohnt sich ein Blick auf die Seite https://haveibeenpwned.com/. Aktuell

Verschiedene Schnittstellen.

sind dort 12,5 Milliarden Accounts aufgeführt, die in einem Hacker-Angriff kompromittiert wurden.

Alternativen zum Passwort

Es gibt aber auch Alternativen zum Passwort. Der Standard FIDO2 (Fast Identity Online) ist schon länger verfügbar. Dabei kommt ein Hardware-Schlüssel zum Einsatz. Wie auf dem Bild ersichtlich, werden verschiedene Schnittstellen unterstützt: USB-A, USB-C, Lightning (iPhone/iPad) oder NFC (Near Field Communication, Funkschnittstelle).

In den Startlöchern steht zudem FIDO Multi-Device-Credentials, oder kurz als Passkey bezeichnet. Es wird anstelle des Hardware-Tokens der PC oder das Handy genutzt. Google hat Anfang Mai damit begonnen, alle Logins auf dieses Verfahren umzustellen. Andere werden sicherlich bald folgen. Passkeys verwenden kryptografische Schlüssel. Ein Passkey besteht aus einem asymmetrischen Schlüsselpaar (einem öffentlichen und privaten Schlüsselteil), das beim Anlegen eines Kontos automatisch erzeugt wird. Der öffentliche Schlüssel wird zum Dienstanbieter übertragen, der private Schlüssel bleibt im Sicherheitschip auf dem Handy oder PC gespeichert. Bei der nächsten Anmeldung auf der Webseite, wird eine mit dem öffentlichen Schlüssel verschlüsselte Aufgabe verschickt, die nur der private Schlüssel mit einer passenden Antwort lösen kann. Das alles läuft im Hintergrund ab. Damit kein Missbrauch durch eine fremde Person erfolgen kann, muss dieser Vorgang per Gesichtserkennung oder Fingerabdruck-Scan bestätigt werden. Unter https://passkeys.directory/ sind einige Anbieter aufgelistet. Laufend kommen weitere dazu.

Ein privater Passkey-Schlüssel lässt sich nicht erraten oder durch Ausspionieren von privaten Informationen ermitteln. Eine gefälschte Webseite, die heute ganz einfach ein Passwortfeld nachbauen kann, wird mit der kryptografischen Anmeldung nicht mehr funktionieren. Da der private Schlüssel nie an Webseiten oder Apps geschickt wird, kann er dort auch nicht gestohlen werden. Einen kleinen Wermutstropfen gibt es aber. Für die «Bequemlichkeit» der Benutzer, die mehrere Geräte nutzen, wird der private Schlüssel in die Apple, Google und Microsoft Cloud übertragen. Mit der Ende-zu-Ende-Verschlüsselung bei der Übertragung soll das allerdings sicher ablaufen.

Trotz der Alternativen wird es noch ein langer Weg sein, bis keine Kennwörter mehr genutzt werden. Erst wenige Anbieter unterstützen die neuen Technologien FIDO2 oder Passkeys. Am weitesten ist Apple, wobei die Verfügbarkeit derzeit auf die eigenen Geräte beschränkt ist. Windows- und Android-Nutzer können mit Chrome-Passkeys nutzen. Doch auch wenn diese Technologie verbreitet genutzt werden kann, bleibt eine Herausforderung bestehen: Nutzer mit vielen Passwörtern wartet eine Menge Arbeit, diese auf Passkeys umzustellen.