Wumbel®

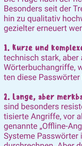
Passwörter - Sind sie sicher?

S-CON

Wussten Sie, dass Ihr Passwort das Einzige ist, was zwischen Ihnen und einem Cyberangriff steht?

Ein typischer Morgen im Büro: Noch schnell den Laptop aufgeklappt, den ersten Kaffee neben die Tastatur gestellt. Schon kann der Tag kann beginnen. Ein Login-Fenster erscheint. **Passwort?** Natürlich dasselbe wie immer. Irgendwas mit dem Namen des Hundes, kombiniert mit der alten Postleitzahl. Leicht zu merken und eigentlich auch völlig harmlos, oder? **Falsch gedacht.**

Was für Sie Alltag ist, ist für Angreifer ein gefundenes Fressen. Denn genau diese Muster, Namen, Orte, Zahlenfolgen, stehen ganz oben auf den automatisierten Listen der Angreifer. Und der **Schaden kann gravierend sein: Identitätsdiebstahl, Kurfchädigung, der Ingriff auf vertrauliche Unternehmensdaten.** Und in manchen Fällen reicht ein einziges gehacktes Passwort aus, um gleich mehrere Systeme zu kompromittieren.



Was ist aktuell besonders wichtig? Die Empfehlungen des BSI:

Das Bundesamt für Sicherheit in der Informationstechnik (**BSI**) hat aufgrund der Bedrohungslage durch Cyberangriffe seine Mindestanforderungen zur Passwortsicherheit aktualisiert. Passwortschutz ist heute mehr als eine Empfehlung. Er ist ein organisatorisches Schutzschild.

Zwei Strategien führen zum Ziel:
1. Kurz und komplex:
- 8-12 Zeichen,
- vier Zeichenarten (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen)
Beispiel: fgfhwlp#

2. Lang und merkbar:
- Mindestens 21 Zeichen,
- zwei Zeichenarten reichen
Beispiel: KaffeeTreppe+Blumen&Eimterbank

Für beide Strategien gilt: Nie doppelt nutzen, pro Account immer ein eigenes Passwort.

Wie oft sollten Sie Ihr Passwort ändern und wovon hängt das ab?

Die Frage nach der richtigen Änderungsfrequenz stellt sich vielen. Besonders seit der Trend weggeht **vom "alle 90 Tage"-Grundsatz** hin zu qualitativ hochwertigen Passwörtern, die seltener, dafür aber gezielter erneuert werden.

1. Kurze und komplexe Passwörter mit vier Zeichenarten sind zwar technisch stark, aber anfälliger für sogenannte Brute-Force- und Wörterbuchangriffe, wenn sie in falsche Hände geraten. Daher sollten diese Passwörter in einem kürzeren Intervall geändert werden.

2. Lange, aber merkbare Passwörter sind besonders resistent gegen automatisierte Angriffe, vor allem gegen sogenannte „Offline-Angriffe", bei denen Systeme Passwörter im Hintergrund durchrechnen. Aber durch die höhere Wahrscheinlichkeit von Eingabefehlern sind sie beim Nutzer häufig unbeliebter. Eine Änderung kann hier jedoch seltener durchgeführt werden. Die Sicherheit eines Passworts hängt vor allem vom Suchraum ab, also der Zahl möglicher Kombinationen.

Beispiel:
Ein Passwort mit 8 Zeichen und 4 Zeichenarten ergibt rund 6 Billiarden Kombinationen. Ein Passwort mit 24 Zeichen (z. B. 4 Wörter à 6 Buchstaben) ergibt mehr als 10^{40} mögliche Kombinationen. Dies ist ein Vielfaches dessen, was ein Rechner sinnvoll durchprobieren könnte.

Hinzu kommt: Lange Passwörter lassen sich leichter merken, wenn sie z. B. aus bildhaften Begriffen bestehen. Das reduziert das Risiko von Zettelnotizen oder unsicheren Speicherorten.

Wann sollte ich mein Passwort sofort ändern?

- Verdacht auf Phishing, Datenleck oder Angriff
- Verdächtige Kontoaktivitäten
- Passwort wurde (versehentlich) weitergegeben

Sichere Passwörter oder "Was man bitte nicht mehr tun sollte!"

Hier sind einige Klassiker, die leider immer noch zu häufig vorkommen:
- 123456, Passwort, **qwertz**
- Anna2012 – (**Name + Geburtsjahr**)
- Hallo!2023 – (**wird von vielen Systemen als stark akzeptiert ist es aber nicht**)
Das gleiche Passwort für E-Mail, Online-Banking, Social Media und Kran kenkassen-App.

Solche Kombinationen sind nicht nur leicht zu erraten, sie sind das Ersetzt, was sogenannte Credential-Stuffing-Angriffe ausprobieren. Vermeiden Sie daher diese Kombinationen.
Übrigens: Auch Zettel unter der Tastatur, gespeicherte Logins im Browser oder der berühmte Screenshot mit den Zugangsdaten zählen zu den größten Schwachstellen im Alltag.

Ein Passwort - was soll schon passieren?

Tatsächlich eine ganze Menge.
Kürzlich wurde ein großer Anbieter von DNA-Tests gehackt, und zwar durch ein einfaches Prinzip: Nutzer verwenden dasselbe Passwort für mehrere Dienste. Angreifer hatten aus unbekannter Quelle ein Passwort abgegriffen und probierten es automatisiert auf einer Vielzahl von Konten aus. Bingo! Plötzlich hatten sie Zugriff auf persönliche Daten, sogar auf Familienverknüpfungen und genetische Informationen. Und das nur, weil jemand sein Passwort „recycelt" hatte.
Das zeigt: Es braucht gar keinen gezielten Angriff. Manchmal reicht ein altes Passwort, das irgendwo im Netz herumgeistert.

5 einfache Tipps für mehr Sicherheit

1. Nutzen Sie für jeden Zugang ein anderes Passwort.

2. Verwenden Sie einen Passwortmanager, so müssen Sie sich nur eines merken.

3. Verzichten Sie auf Browserfunktionen wie „Passwort speichern".

4. Aktivieren Sie, wenn möglich, eine Zwei-Faktor-Anmeldung (z. B App, SMS, PIN)

5. Überprüfen und ändern Sie Ihre Passwörter regelmäßig.

Und falls Sie mal überlegen: Wer sollte ausgerechnet mich hacken?

Denken Sie an den Gentestanbieter. Niemand war persönlich gemeint und trotzdem waren Millionen betroffen.

Denn das Problem ist nicht, dass man es speziell auf Sie abgesehen hat, sondern, dass Ihr Passwort so leicht zu knacken ist.

Wumbel

S-CON GmbH & Co. KG
Podbielskistraße 386
30659 Hannover

S-CON

Servicenummer: 0800 88446688
E-Mail: office@s-con.de