LU07b - Passwörter

Die Verwendung von Passwörtern ist seit längerer Zeit umstritten. Dies liegt daran, dass viele Benutzer immer die gleichen und oft zu einfachen Passwörter verwenden.

Passwort-Richtlinien

Viele Firmen und Webseiten versuchten (und versuchen) durch Passwort-Richtlinien das Problem in den Griff zu bekommen. Dabei sind vor allem diese Regeln im Einsatz:

- Komplexe Passwörter:
  - Das Passwort muss eine minimale Länge haben, zum Beispiel >= 8 Zeichen.
  - Das Passwort muss Klein-, Grossbuchstaben, Ziffern und Sonderzeichen enthalten.
  - Das Passwort darf weder den Vor- noch den Nachnamen enthalten.
  - Das Passwort darf keine Liste von Buchstaben (z.B. cdefghijk) noch Ziffern (z.B. 123456) sein.
- Passwort wechseln:
  - Das Passwort muss regelmässig, z.B. alle 3 Monate geändert werden.
  - Das neue Passwort darf nicht mit den zwei letzten Passwörtern übereinstimmen.

Es gibt Untersuchungen die zeigen, dass diese Passwort-Richtlinien zu schlechteren Passwörtern führen. Wenn ich mir alle 3 Monate ein neues, 8 stelliges Passwort merken muss, nehme ich ein möglichst einfach zu merkendes Passwort.

Sichere Passwörter

Damit Passwörter sicher sind, müssen sie einige Kriterien erfüllen:

- Mindestens 8 Zeichen lang
- Buchstaben, Ziffern und Sonderzeichen enthalten
- Nur für ein Benutzerkonto verwenden
- Keine Wortkombinationen, Zahlen- oder Buchstabenreihen enthalten

Am sichersten sind Passwörter, die aus einer zufallsgenerierten Abfolge von Zeichen bestehen. Doch wie soll ich mir 100 oder mehr solcher Zufallspasswörter merken?

Passwörter mit System

Bei dieser Variante verwende ich eine gemeinsame Logik für alle Passwörter. Zum Beispiel verwende ich einen Satz, den ich mir gut merken kann. Für jedes Login verwende ich einen Teil dieses Satzes und ergänze ihn.

Beispiel

Nehmen wir dieses Zitat aus Dirty Harry: *You've got to ask yourself one question: „Do I feel lucky? Well, do ya, punk?“*

Ich möchte nun ein Passwort für den Webshop von Emutech erzeugen.

- Am Anfang stelle ich die erste Hälfte des Webshopnamens: `Emut`
- Anschliessend folgt die Ziffer 5 und ein Sonderzeichen @
- E ist der 5. Buchstabe im Alphabet, daher nehme ich jedes 5. Wort: `askIya`
- Ans Ende stelle ich die zweite Hälfte des Webshopnamens: `ech`

Mein Passwort wäre nun: `Emut5@askIyaech`

Passwortkarte

Quelle: chip.de

Eine Passwortkarte besteht aus zufällig generierten Zahlen und Buchstaben. Um ein sicheres Passwort zu erhalten, merke ich mir

- Eine Lesemethode wie sie in den rot umrandeten Beispielen gezeigt werden.
- Einen Startpunkt für jedes Benutzerkonto, welchen ich sogar auf der Rückseite der Karte notieren könnte.

Siehe auch https://www.savernova.com/loesungen/sichere-passwortkarte

Der Vorteil eine Passwortkarte ist, dass die Passwörter sicher vor jedem Hackangriff sind. Um an meine Passwortkarte zu gelangen, müsste man diese aus meiner Brieftasche stehlen.

Passwortmanager

Ein Passwortmanager oder Passwortsafe ist eine Software, welche meine Passwörter in einer verschlüsselten Datenbank speichert. Der Passwortmanager kann eine selbständige Software (z.B. Keepass) oder in einen Webbrowser (z.B. Firefox Password Manager) sein. Neben dem sicheren Speichern der Passwörter bieten viele Passwortmanager weitere Funktionen wie das automatische

Ausfüllen von Loginformularen.

Passwortmanager im Vergleich 2023

chip.de - Vergleichstest

Das Ende der Passwörter

Als Betreiber einer Webseite oder Netzwerks können wir unsere Benutzer nicht zu sicheren Passwörtern zwingen. Wieso schaffen wir die Passwörter nicht einfach ab? Tatsächlich arbeiten verschiedene Technologiefirmen genau daran. Im Mai 2023 machte Google Schlagzeilen: 20min - Google will das Passwort abschaffen.

Lesen Sie dazu chip.de - Es geht auch ohne Passwörter

---

m231-AnG