A1 Business

Das Problem mit dem Passwort

A1. Verantwortung für Ihr Business.

Schwache Passwörter

Viele Nutzer verwenden bei Einrichtung ihrer digitalen Identität bei einem Dienst im Internet schwache Passwörter

- Grund: „Menschlicher Faktor“ („Human Factor“)
  - Bequemlichkeit
  - Komplexe Passwöter sind schwer zu merken
  - Fehlendes Sicherheitsbewusstsein
  - …
- Passwörter können aus verschiedenen Gründen schwach sein:
  1. Zu geringe Komplexität
  2. Ableitbar aus Nutzerkontext
  3. Wiederverwendung bereits genutzter Passwörter

Schwache Passwörter: Passwörter mit geringer Komplexität

Wann sind Passwörter schwach:

- Weniger als 12 Zeichen
- Verwendung nur einer Zeichengruppe (Zahlen, Buchstaben, Sonderzeichen)
- Tastenfolge auf Tastatur, z.B. „qwertz", „qwe123", ...
- Auffindbar in einem Wörterbuch
- Kriterien für „starke" Passwörter können abweichen

#	Passwort	Häufigkeit
1	123456	8,01%
2	123456789	3,84%
3	password	1,87%
4	qwerty	1,82%
5	12345	1,36%
6	12345678	1,15%
7	111111	1,14%
8	qwerty123	1,00%
9	1q2w3e	0,95%
10	123123	0,84%

Top 10 der meistgenutzten Passwörter basierend auf Klartext-Leaks im HPI Identity Leak Checker

Schwache Passwörter: Wiederverwung von Passwörtern

Viele Nutzer verwenden persönliche Daten als Passwörter

- Name, Vorname, Name des Partners / Kindes / Elternteils
- Geburtsdatum
- Lieblingsband oder Fußballverein
- …

Teilweise werden Passwörter auch nach jeweilig genutztem Dienst gewählt

- Adobe Datenbank: adobe123, photoshop, adobe1, …

→ Angreifer, der sein Opfer kennt, kann solche Passwörter leicht erraten

Schwache Passwörter: Passwörter aus dem Nutzerkontext

Viele Nutzer verwenden relativ sichere Passwörter, aber gleiches Passwort wird oft für verschiedene / alle Accounts verwendet, z.B.

- zU-&l8e0iJ&A wird bei der Anmeldung für jeden Dienst verwendet

→ **Wird Passwortdatei nur eines Dienstes geleakt, dann sind auch alle anderen Dienste betroffen**

Wird Passwort nur leicht abgewandelt für unterschiedliche Accounts verwendet, kann das zu schnellerem Erraten führen

- zU-&l8e0iJ&A für Dienst A
- zU-&l8e0iJ&B für Dienst B
- ...

Wahl eines sicheren Passwortes

- Keine Informationen aus dem **Nutzerkontext** verwenden, also keine Informationen, die Angreifer über ihr Opfer recherchieren können
- Keine Wörter aus einem **Wörterbuch** oder **Sprichwörter**
- Mindestens **12 Zeichen** lang
- Passwortzeichen aus **verschiedenen Zeichengruppen** wählen (Sonderzeichen, Groß-und Kleinbuchstaben, Ziffern)
- Verwendung **unterschiedlicher Passwörter** für unterschiedliche Accounts
- Keine Wiederverwendung alter Passwörter
- Eventuell Passwortmanager nutzen