

openHPI-Kurs „Digitale Identitäten“
Angriffe auf Accounts – Schwache Passwörter

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Schwache Passwörter

Viele Nutzer verwenden schwache Passwörter für Dienste im Internet

Grund: „Menschlicher Faktor“ (Human Factor)

- Bequemlichkeit
- fehlendes Sicherheitsbewusstsein
- komplexe Passwörter sind schwer zu merken
- ...

Passwörter können aus verschiedenen Gründen schwach sein

1. Passwörter **geringer Komplexität**
2. Passwörter mit **Herleitung aus Nutzerkontext**
3. **Wiederverwendung** von Passwörtern

Schwache Passwörter: Passwörter mit geringer Komplexität

Wann sind Passworte zu einfach?

- < 12 Zeichen
- Verwendung nur einer Zeichengruppe (Zahlen, Buchstaben, Sonderzeichen)
- Auffindbar in einem Wörterbuch
- Tastenfolge auf Tastatur, z.B. „qwertz“, „qwe123“, ...

Passwort	Häufigkeit
123456	1,19%
123456789	0,52%
12345678	0,35%
12345	0,19%
password	0,15%
111111	0,11%
11111111	0,10%
123123	0,09%
1234567	0,08%
000000	0,07%

Quelle: HPI Identity Leak Checker

Tabelle zeigt **Top 10 Passwörter** aus Datenbank des HPI Identity Leak Checkers

Schwache Passwörter: Passwörter aus dem Nutzerkontext

Viele Nutzer verwenden **persönliche Daten als Passwörter**

- Nutzernamen: Name, Name des Partners / Kindes / Elternteils
- Geburtsdatum, Geburtsdatum des Partners / Kindes / Elternteils
- ...

Teilweise wird Passwort auch **vom authentifizierenden Dienst abgeleitet**

- Adobe Datenbank: adobe123, photoshop, adobe1, ...
- Angreifer, der sein Opfer kennt, kann derartige Passwörter leicht erraten

Schwache Passwörter: Wiederverwendung von Passwörtern (1/2)

Viele Nutzer verwenden relativ sichere Passwörter

Aber:

Gleiches Passwort wird oft für viele Accounts verwendet, z.B.

- Passwort ***D7\$4?g!inRo***
 - leicht abgewandeltes Passwörter wird für unterschiedliche Accounts, z.B.
 - ***D7\$4?g!inRoA*** für Dienst A, ***D7\$4?g!inRoB*** für Dienst B,
D7\$4?g!inRoC für Dienst C
- Wird Passwortdatei nur eines Onlinedienstes geleakt und landet im Internet, dann sind auch alle anderen Dienste betroffen ...

Schwache Passwörter: Wiederverwendung von Passwörtern (2/2)

Problem: 63% von Datendiebstählen sind unsachgemäßer Passwortnutzung geschuldet (Verizon Breach Report, 2016)

- Kritisch ist vor allem die Passwortwiederverwendung

Untersuchen von über 1 Milliarde Nutzer-Passwörter aus dem HPI ID-Leak Checker zeigen:

- 68 Millionen Nutzer hatten mindestens zwei Accounts
- Beobachtung
 - **20%** der Nutzer verwenden **identische Passwörter** mehrmals
 - **27%** der Nutzer verwenden **ähnliche Passwörter** mehrmals
 - Aber: Bei **ähnlichen Diensten** liegt Wiederverwendung bei teils **50%**

Eigenschaften sicherer Passwörter

- Keine Informationen aus dem **Nutzerkontext**, also keine Informationen, die Angreifer über ihr Opfer recherchieren könnten
 - z.B. Nutzernamen, Name, Geburtsdatum, ...
- Keine Wörter aus einem **Wörterbuch** oder Sprichwörter
- Mindestens **12 Zeichen**
- Gebildet aus verschiedenen **Zeichengruppen** (Sonderzeichen, Groß- und Kleinbuchstaben und Ziffern)
- Verwendung **unterschiedlicher Passwörter** für Accounts und keine Wiederverwendung alter Passwörter
- Einhaltung dieser Regeln erschwert erheblich den Missbrauch sämtlicher Accounts

Zusammenfassung: Schwache Passwörter

■ Problem

- viele Nutzer wählen wegen fehlendem Sicherheitsbewusstsein und aus Bequemlichkeit schwache Passwörter (**Human Factor**)
- schwache Passwörter lassen sich leichter merken, können aber auch schnell erraten oder geknackt werden

■ Schwache Passwörter

- haben eine geringe Komplexität
- lassen sich aus dem Nutzerkontext ableiten

■ Passwortwiederverwendung

- wiederverwendete Passwörter gelten als schwach
- wenn ein (starkes) Passwort im Klartext geleakt wird, sind alle Accounts mit dem gleichen Passwort gefährdet