Lisa Braune und EUROKEY Software GmbH
06.05.2024

Passwortsicherheit

Sichere, Merkbare Passwörter ausdenken

1. **Satz ausdenken** (mind 8 Wörter)
2. **Anfangsbuchstaben rausschreiben**
3. **Sonderzeichen und Buchstaben einstreuen** (oder schon im Satz Zahlen und Sonderzeichen beinhalten)

Das sollten Sie tun:

- Passwörter ändern nach einem **Leak** und **Standardpasswörter**
- **Passwort-Manager** benutzen
- **2-Faktor-Authentifizierung** benutzen

Das sollten Sie nicht tun:

- Passwörter aufschreiben
- Passwörter an Andere weitergeben (auch nicht an Chefs, Kollegen, Freunde oder IT)
- Dasselbe Passwort für unterschiedliche Dienste verwenden

Leak = Passwörter oder persönliche Daten wurden in Umlauf gebracht, z.B. nach einem Hack

➔ Leakcheck für die Mailadresse: ‣ have i been pwned
➔ Leakcheck auf persönliche Daten: ‣ HPI Identity Leak Checker
➔ Leackcheck von Handynummer, Bankkarten, Ausweise: ‣ SCHUFA IdentChecker

Passwort-Manager = ein Tresor für die eigenen Passwörter, um diese sicher abzuspeichern. Der Schlüssel für den Tresor ist das Masterpasswort

➔ Kostenloser PW-Manager: ‣ KeePass

2-Faktor-Authentisierung = sich zweifach ausweisen, um sich einzuloggen (z.B. mit Passwort und Code per SMS)

Wie Hacker an Passwörter kommen

1. **Brute Force** (deutsch „Rohe Gewalt“) = Technik, um an Passwörter zu kommen. Dabei werden alle möglichen Kombinationen automatisiert ausprobiert. Je länger und mehr verschiedene Zeichen das Passwort, desto länger dauert das Knacken

Beispiel:

Passwort: „sjwmclod“	Passwort: „jA1c-8mJ“
- 8 Zeichen - Nur Kleinbuchstaben - **In 21 Sekunden geknackt!**	- 8 Zeichen - Klein- und Großbuchstaben, Zahlen, Sonderzeichen - **In 8 Tagen geknackt!**

➔ Passwort auf Sicherheit prüfen: ‣ checkdeinpasswort.de/

1. **Häufige Passwörter, Namen, Daten und Wörter ausprobieren** = Technik, um an Passwörter zu kommen. Dabei werden die Einträge Listen mit häufigen Passwörtern, Namen, Daten und Wörtern miteinander kombiniert und ausprobiert. Geht sehr viel schneller als Brute Force

➔ **Listen häufiger (und unsicherer) Passwörter:** ‣ Wikipedia