

# Passwörter & MFA — vom Risiko zur Verteidigung

Mehr als drei Viertel aller Datenlecks involvieren kompromittierte oder schwache Zugangsdaten. Wir erklären den Stand der Technik 2026 — Passkeys, FIDO2, MFA-Müdigkeit — und was Mitarbeitende davon konkret tun müssen.

min Lesezeit: 8 min    Aktualisiert: 14. März 2026    Risiko: Hohes Risiko  
Quelle: [awareness-as-a-service.com/de/resources/threats/passwords-mfa](https://awareness-as-a-service.com/de/resources/threats/passwords-mfa)

## Was sind Passwörter & MFA — und warum sind sie kritisch?

Das Passwort ist seit Jahrzehnten das schwächste Glied in der Sicherheitskette — und gleichzeitig dasjenige, das am häufigsten ausgenutzt wird. **Kompromittierte oder schwache Zugangsdaten** sind laut Verizon DBIR in mehr als drei Viertel der Datenlecks beteiligt. Wer Zugangsdaten besitzt, braucht keine Schadsoftware.

**Multi-Faktor-Authentifizierung (MFA)** wurde als Gegenmittel eingeführt: Wer neben dem Passwort einen zweiten Faktor (Code, Push-Bestätigung, Hardware-Token) vorweisen muss, ist gegen reine Passwort-Kompromittierung geschützt. Doch

Angreifer haben sich angepasst: **MFA-Fatigue** (auch Push-Bombing genannt) hat sich als eigene Angriffstechnik etabliert — Angreifer senden massenweise Push-Bestätigungen, bis der genervte Nutzer eine davon bestätigt.

2026 rückt die passwortlose Zukunft näher: **Passkeys** (FIDO2/WebAuthn) ersetzen Passwörter durch kryptografische Schlüsselpaare, die phishing-resistent, gerätegebunden und nicht rück-entschlüsselbar sind. Große Plattformen (Microsoft, Google, Apple) unterstützen sie bereits produktiv.

## Auf einen Blick

01

### Passwort-Wiederverwendung ist das grösste Risiko

Wer dasselbe Passwort auf mehreren Seiten nutzt, riskiert, dass ein einziges Datenleck alle anderen Konten öffnet. Credential Stuffing nutzt genau das aus.

02

### MFA ist kein Allheilmittel

SMS-OTP ist schwächer als App-basierte TOTP, die wiederum schwächer ist als FIDO2/Passkeys. MFA-Fatigue und Adversary-in-the-Middle-Angriffe umgehen SMS und App-Push.

03

### Passkeys sind 2026 praxistauglich

Für viele Unternehmensanwendungen sind FIDO2/Passkeys bereits verfügbar. Sie bieten phishing-Resistenz, da sie an die Domain gebunden sind und nicht an eine gefälschte weitergegeben werden können.

## Woran erkennen Sie typische Passwort-Risiken?



### Passwort-Wiederverwendung

Mitarbeitende nutzen ihr Unternehmenspasswort auch für private Dienste. Ein Datenleck bei einem der privaten Dienste öffnet das Unternehmenskonto.



### Passwörter auf Post-its oder in Klartextdateien

Handgeschriebene oder digital ungeschützt gespeicherte Passwörter sind für jeden zugänglich, der physischen oder digitalen Zugang zum Arbeitsplatz hat.



### MFA-Müdigkeit (Push-Bombing)

Wer eine unerwartete MFA-Push-Anfrage erhält, die er selbst nicht ausgelöst hat, sollte diese ablehnen — nicht aus Bequemlichkeit bestätigen.



### Account-Sharing

Gemeinsam genutzte Konten (z.B. Social-Media-Accounts des Unternehmens) können nicht individuell gesperrt und nach einem Austritt nicht sauber getrennt werden.



### Schwache Passwortrichtlinien

"Passwort1!" erfüllt viele formale Anforderungen (Groß, Klein, Zahl, Sonderzeichen) ist aber trivial zu erraten. Richtlinien, die nur Komplexität fordern, aber keine Länge, schaffen Scheinsicherheit.

## So schützen Sie sich

### Für Mitarbeitende

- **Passwort-Manager einsetzen:** Einen einzigartigen, langen Zufalls-String pro Konto — der Manager merkt sich alles. Empfehlenswert: Bitwarden, 1Password, KeePassXC.
- **MFA überall aktivieren**, wo verfügbar — zumindest App-basierte TOTP (Google Authenticator, Aegis). Passkeys aktivieren, wenn angeboten.
- **Unerwartete MFA-Push-Anfragen ablehnen und melden.** Sie selbst haben sich nicht angemeldet — also kommt die Anfrage von jemand anderem.
- **Passwörter nie weitergeben** — auch nicht an IT-Helpdesk oder Vorgesetzte. Kein legitimes

System fragt danach.

- **Passwörter regelmäßig ändern, wenn Verdacht auf Kompromittierung besteht** — nicht aus reiner Routine (das führt zu schwächeren Passwörtern durch Vorhersehbarkeit).

### Für Administratoren

- **FIDO2/Passkeys für alle kritischen Systeme** rollout-planen — Microsoft Entra, Okta, Ping Identity und andere IAM-Plattformen unterstützen das bereits produktiv.
- **MFA-Fatigue-Schutz aktivieren:** Number Matching (Nutzer muss eine angezeigte Zahl bestätigen) und Additional Context (Standort, App-Name) in der Push-Konfiguration einschalten.

- **Passwort-Spraying- und Credential-Stuffing-Schutz:** Account-Lockout-Richtlinien, Anomalie-Erkennung bei ungewöhnlichen Login-Geografien, HIBP-Abgleich bei Passwortänderungen.
- **Privilegierte Konten besonders schärfen:** Admin-Konten bekommen FIDO2, keine SMS-MFA, keine geteilten Accounts.
- **Passwort-Manager als Unternehmensstandard** bereitstellen — so senken Sie die Hürde für gutes Verhalten.

## Echte Beispiele

FALL 01 · VERSICHERUNGSGESELLSCHAFT · DE · Q2/2025

Credential-Stuffing-Angriff auf das Kundenportal: Angreifer nutzten eine Liste aus einem Datenleck eines Fitness-Apps und probierten dort verwendete E-Mail/Passwort-Kombinationen durch. Mehrere hundert Kundenkonten wurden innerhalb einer Nacht übernommen.

**Schaden:** Kundendaten kompromittiert, Regulierungsmeldung nach DSGVO erforderlich · **Erkennung:** Anomalie-Erkennung schlug nach Stunde 3 an · **Lehre:** Rate-Limiting und HIBP-Integration bei Anmeldung hätten den Angriff deutlich früher blockiert.

FALL 02 · NPO · CH · Q1/2026

Ein Mitarbeiter bestätigte aus Gewohnheit eine MFA-Push-Anfrage um 2:07 Uhr — ohne nachzudenken. Der Angreifer hatte das Passwort aus einem alten Datenleck und sendete Push-Anfragen, bis eine bestätigt wurde. Über das kompromittierte Konto wurden Spenderdaten und Finanzberichte heruntergeladen.

**Schaden:** Datenschutzverletzung, Vertrauen von Großspendern gefährdet · **Erkennung:** Benutzer meldete sich am nächsten Morgen wegen Kontozugriffsproblemen · **Lehre:** Number Matching hätte eine zufällige Bestätigung verhindert.

## Was tun, wenn es passiert ist?

### DIE ERSTEN 15 MINUTEN

1. **Passwort sofort ändern** — von einem nicht kompromittierten Gerät aus.
2. **Alle aktiven Sessions invalidieren** (bei den meisten Diensten: "Alle Geräte abmelden").
3. **IT-Security oder ISB informieren** — besonders wenn ein Unternehmenskonto betroffen ist.
4. **MFA-Geräte prüfen:** Wurden ohne Ihr Wissen neue Geräte oder Apps als zweiter Faktor registriert?
5. **Andere Konten mit gleichem Passwort prüfen** und dort sofort ebenfalls ändern.
6. **HIBP-Abgleich (haveibeenpwned.com):** Prüfen, ob Ihre E-Mail-Adresse in bekannten Datenlecks vorkommt.

## Häufige Fragen

### Wie lang sollte ein sicheres Passwort sein?

Mindestens 16 Zeichen, wenn es sich noch um ein klassisches Passwort handelt. Länge ist wichtiger als Komplexität: "Kaffee-Montag-Blau-42" ist sicherer als "P@ssw0rd!". Noch besser: Einen Passwort-Manager zufällige 24-Zeichen-Strings generieren lassen.

### Was ist der Unterschied zwischen TOTP und FIDO2?

TOTP (Time-based One-Time Password, z.B. Google Authenticator) generiert alle 30 Sekunden einen neuen Code — der kann aber durch einen Angreifer in Echtzeit abgefangen und weitergeleitet werden (Adversary-in-the-Middle). FIDO2/Passkeys sind domain-gebunden: Eine gefälschte Website kann den Schlüssel nicht nutzen, weil die Domain-Prüfung im Protokoll verankert ist.

**Darf IT das Passwort eines Mitarbeiters kennen?**

Nein. Passwörter sollten nur dem Nutzer bekannt sein und beim Anbieter nur als Hash gespeichert werden. Wenn IT Passwörter zurücksetzen muss, geschieht das über einen Reset-Prozess — nicht über Kenntnis des aktuellen Passworts.

**Sind Passwort-Manager selbst sicher?**

Kommerzielle Passwort-Manager (Bitwarden, 1Password) werden von Sicherheitsexperten empfohlen und regelmäßig auditiert. Das Risiko aus einem einzigen kompromittiertem Master-Passwort ist real — weshalb das Master-Passwort selbst stark sein und nur für den Manager verwendet werden sollte. MFA auf dem Manager-Konto ist Pflicht.

**Weitere Themen**

---

Schwache Zugangsdaten sind der Einstieg für Phishing, CEO-Fraud und Deepfake-gestützte Angriffe. KI-basierte Angriffe machen Passwort-

Kompromittierung noch schneller und überzeugender.