Passwörter – Was soll schon schiefgehen?

Thomas Heinz, Juli 2025

Was wollen Hacker mit meinem Passwort?

- Login-Daten als Eintrittskarte zu deinem Bankkonto.
- Als Einstiegspunkt in das persönliche Konto einer Person können böswillige Akteure deine anderen Online-Konten hacken. Das ist einfach, wenn du das gleiche Passwort für verschiedene Konten verwendest.
- Identitätsdiebstahl oder Finanzbetrug
  dies kann in Form von illegalen Käufen, Geldüberweisungen oder der Geiselnahme deiner Daten durch Ransomware geschehen.
- Straftaten in deinem Namen verüben, z.B.
  Verkauf nicht existierender Waren gegen Vorkasse (Betrug).
  Es gab auch Fälle, dass Beträge über die Handyrechnung abgebucht wurden.
- Sich online als dich ausgeben: Wenn ein Hacker vollen Zugriff auf dein E-Mail-Konto erhält, kann er in der Regel die meisten deiner sensiblen Daten finden oder einen Weg, auf sie zuzugreifen.
- Deine Kontakte sind dadurch auch betroffen, indem sie Phishing Mails von deinem Account erhalten.

Welche Arten von persönlichen Daten sind für Hacker am wertvollsten?

Hacker sind auf der Suche nach persönlichen Daten, die für Finanzbetrug, Identitätsdiebstahl oder den gewinnbringenden Weiterverkauf genutzt werden können. Zu den wertvollsten Datenarten gehören:

- Sozialversicherungsnummern
- Kreditkartendaten
- Bankkontoinformationen
- Anmeldedaten
- Gesundheitsdaten
- E-Mail-Adressen
- Führerschein- oder Passdaten

Wie werden Passwörter geknackt?

Was wir also brauchen, sind Passwörter, die

- Nicht zu erraten sind
- Nicht zu knacken sind
- Leicht zu merken sind

Dazu hilft zu wissen, wie Passwörter gehackt werden. Da sitzt natürlich niemand in einem dunklen Zimmer an einem Computer und tippt ein Passwort nach dem nächsten ein. Das erledigen Programme auf leistungsfähiger Hardware.

Brute Force attack

Dieser Ansatz ist der simpelste, aber auch ein recht ineffizienter Weg.

Bei einer Brute-Force-Attacke werden alle möglichen Kombinationen von Buchstaben, Zahlen und Sonderzeichen ausprobiert. Es erfolgt also kein zielgerichteter Angriff, sondern, wie der Name schon sagt, ein Versuch mit „roher Gewalt“.

Mit zunehmender Passwortlänge steigt der Aufwand exponentiell an. Da die Leistung moderner Hardware immer mehr steigt und sich der Zeitaufwand für das Durchprobieren dadurch erheblich reduziert, muss die minimale Passwortlänge ausreichend groß gewählt werden.

Die Methode ist in der Praxis häufig erfolgreich, da die meisten Nutzer kurze und einfache, damit unsichere Passwörter verwenden.

Dictionary attack

Dies ist eine verfeinerte Brute-Force-Variante, bei der Hacker Wörterbücher (engl. dictionary) mit gebräuchlichen Wörtern, Formulierungen und Institutionen wie Sportmannschaften, Firmen usw. erstellen. Dadurch wird die Liste der möglichen Passwörter eingegrenzt.

Wer seine Lieblings-Fußballmannschaft in sein Passwort einbaut, hat hier schnell das Nachsehen.

Die einzige Verteidigung des Nutzers gegen einen Wörterbuchangriff ist, keine leicht erratenbare Passwörter zu verwenden.

Mask attack

Für die Erstellung von Kennwörtern werden Muster eingesetzt, welche häufig aus verfügbaren Sammlungen gehackter anderer Passwörter im Darknet stammen. Mit diesen Mustern erstellt der Hacker einen Filter (oder eine “Maske”) und wendet diesen auf seine Wörterbuchliste an. Auf diese Weise lässt sich die Gesamtzahl möglicher Passwörter, die erraten werden müssen, drastisch reduzieren.

Angreifer nutzen Informationen über die Gewohnheiten bei der Passwort-Erstellung, wie z.B. gängige Zusammensetzungsmuster, um diese Angriffe zu entwickeln.

Mehr Sicherheit bieten hier zufällig generierte Passwörter, die derartige Muster nicht aufweisen.

Credential Stuffing

Die leichtsinnige mehrmalige Nutzung von Anmeldedaten wird beim Credential Stuffing ausgenutzt. Es ist eine Brute-Force-Technik, bei der Anmeldedaten (Credentials), die aus einem erfolgreichen Datenklau stammen, genutzt werden, um sich bei anderen Benutzerkonten des Nutzers anzumelden.

Credential Stuffing beruht auf der Tatsache, dass viele Nutzer gleiche Nutzernamen und Passwörter bei mehreren Diensten gleichzeitig verwenden. Selbst starke Passwörter stellen dann kein Hindernis mehr dar.

Die mehrmalige Nutzung von Passwörtern ist zwar oft eine angenehme, aber auch eine sehr unsichere Angewohnheit.

Man-in-the-Middle attack

Bei Man-in-the-Middle-Angriffen wird die Kommunikation zwischen einem Nutzer und einer Website abgefangen und ausspioniert.

Beispiel: Der Hacker richtet einen kostenlosen, öffentlichen WLAN-Hotspot ein, der von Personen, die ihn für einen offiziellen Hotspot eines Cafés in der Nähe halten, genutzt wird. So lassen sich Online-Aktivitäten leicht ausspionieren.

Nicht umsonst warnen viele Smartphones vor dem Einloggen in öffentliche Hotspots.

Starke Passwörter

97% der unsichersten Passwörter bestehen aus weniger als 12 Zeichen

In unter einer Sekunde können Hacker alle 50 der am meisten verwendeten Passwörter der Welt knacken.

Anzahl Zeichen	Nur Ziffern	Kleinbuchstaben	Klein- und Großbuchstaben	Ziffern, Klein- und Großbuchstaben	Ziffern, Klein- und Großbuchstaben und Sonderzeichen
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	Sofort	Sofort	Sofort
6	Sofort	Sofort	Sofort	1 Sekunde	5 Sekunden
7	Sofort	Sofort	25 Sekunden	1 Minute	6 Minuten
8	Sofort	5 Sekunden	22 Minuten	1 Stunde	8 Stunden
9	Sofort	2 Minuten	19 Stunden	3 Tage	21 Tage
10	Sofort	58 Minuten	1 Monat	7 Monate	5 Jahre
11	2 Sekunden	1 Tag	5 Jahre	41 Jahre	400 Jahre
12	25 Sekunden	21 Tage	300 Jahre	2.000 Jahre	34.000 Jahre
13	4 Minuten	1 Jahre	16.000 Jahre	100.000 Jahre	2 Mio. Jahre
14	41 Minuten	51 Jahre	800.000 Jahre	9 Mio. Jahre	200 Mio. Jahre
15	6 Stunden	1.000 Jahre	43 Mio. Jahre	600 Mio. Jahre	15.000 Mio. Jahre
16	2 Tage	34.000 Jahre	2.000 Mio. Jahre	37.000 Mio. Jahre	1.000.000 Mio. Jahre
17	28 Tage	800.000 Jahre	100.000 Mio. Jahre	2.000.000 Mio. Jahre	93.000.000 Mio. Jahre
18	9 Monate	23 Mio. Jahre	61.000.000 Mio. Jahre	100.000.000 Mio. Jahre	7.000.000.000 Mio. Jahre

„Das Passwort muss mindestens 12 Zeichen lang sein, Klein- und Großbuchstaben sowie Zahlen und Sonderzeichen enthalten“ war lange Zeit eine gängige Forderung an Passwörter. Mit Eselsbrücken und Hilfen wie „Nehmen Sie einen Merksatz und notieren Sie davon die Anfangsbuchstaben. Ersetzen Sie einzelne Buchstaben durch Zahlen oder fügen Sie Zahlen sowie Sonderzeichen hinzu. Aus **Wer reitet so spät durch Nacht und Wind?** wird zunächst ***WrssdNuW?*** und dann ***Wr55dNuW?***“

In den letzten 20 Jahren haben wir so gelernt, Passwörter zu verwenden, die für Menschen schwer zu merken, aber für Computer leicht zu erraten sind.

"Betonampelpalme" lässt sich einfacher merken und ist sehr viel schwieriger zu dechiffrieren als "Wr55dNuW?".

Merke: Das stärkste Kennwort wird schwach, wenn man es sich nicht merken kann!

„Wir erleben eine astronomische Beschleunigung der Rechenleistung“, warnt Hive-Chef Alex Nette in einer Pressemitteilung. „Die KI-Hardware von heute verändert bereits die Cybersicherheitsrisiken. Passwörter, die letztes Jahr noch sicher waren, könnten jetzt in einem Bruchteil der Zeit geknackt werden.“

Bewährte Praktiken für die Passwortstärke

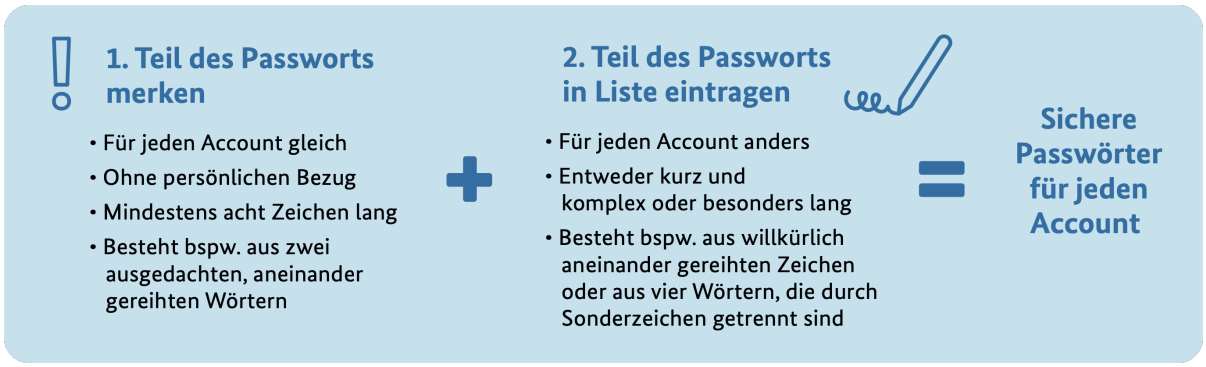
- **Mach es lang!**
  Lange Passwörter sind echt wichtig, um sicher zu sein, dass sie stark genug sind. Ein Passwort mit 8 Zeichen zu knacken, kann schon mal ein paar Minuten dauern. Aber ein Passwort mit 16 Zeichen? Milliarden Jahre!
  In Anbetracht der Entwicklung der Rechenleistung werden mittlerweile 16 Zeichen empfohlen.
- **Mach es zufällig!**
  Pass auf, dass deine Passwörter keinem erkennbaren Muster folgen und eine Mischung aus Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen oder Wörtern enthalten, die nichts mit persönlichen Informationen zu tun haben.

- **Mach es einzigartig!**
  Verwende für jedes deiner Online-Konten ein anderes Passwort. Wenn dann doch mal ein Passwort gehackt wird, ist die Wahrscheinlichkeit geringer, dass die anderen Konten auch betroffen sind.

Das sichere Passwort-Merkblatt

Alle Accounts im Blick

- Diese Methode macht das Passwort-Management im Alltag einfacher! Anstatt viele verschiedene Passwörter zu merken, brauchst du nur noch ein Passwort. Denn bei dieser Methode besteht jedes Passwort aus zwei Teilen.
- Der erste Teil jedes Passworts ist immer gleich. Den musst du dir merken.
- Der zweite Teil ist für jeden Account unterschiedlich. Den trägst du in die Liste ein.
- Wenn Dritte an das Passwort-Merkblatt kommen, kennen sie nur den zweiten Teil des Passworts, nicht aber den ersten. Damit ist das Merkblatt für jede Person außer dir selbst unbrauchbar und deine Accounts sind sicher. Für beide Teile gilt: Beachte die Regeln zur Erstellung eines sicheren Passworts!



Account	Nutzername/ E-Mail-Adresse	2. Teil des Passworts
1. Musteraccount	*maxine@musterfrau.de*	*q7yPv8!x§B2*
2. Musteraccount	*maxine@musterfrau.de*	*Berg_spät_hüpfen_Kühlschrank*

Passwortmanager

Vorteile	Nachteile
Cloudbasiert	Cloudbasiert
Sicher	Teilweise kostenpflichtig
Schnell	
Überwacht Sicherheitsverletzungen	
Macht das Passwort-Management im Alltag einfacher	
Synchronisiert Smartphone, Tablet und Computer	

Browser-gestützte Passwort-Manager (wie Google Chrome, Mozilla Firefox und Microsoft Edge) sind nicht immer so sicher wie dedizierte[1] Passwort-Manager. Wenn du sehr vertrauliche Daten speicherst, ist es besser, einen spezialisierten Passwort-Manager zu verwenden.

Eine kleine (subjektive) Auswahl bekannter Passwortmanager:

Bitwarden

Bitwarden hat Server in Europa, speziell in der EU, die für die Datenspeicherung verwendet werden können. Allerdings ist der Hauptsitz in den USA.

Bietet sowohl kostenlose als auch Premium-Versionen mit starken Sicherheits-funktionen. Laut CHIP bietet Bitwarden eine solide Sicherheitsarchitektur und ist aufgrund des niedrigen Preises der Preis-Leistungs-Sieger.

Pro: Kostenlos.
Con: Hauptsitz in USA.

1Password

1Password hat seinen Hauptsitz in Kanada, nutzt aber auch Cloud-Server, die teilweise in den USA gehostet werden.

Bekannt für seine Benutzerfreundlichkeit und umfangreiche Funktionen, einschließlich der Möglichkeit zur Zwei-Faktor-Authentifizierung. Laut F.A.Z. Kaufkompass bietet 1Password eine hervorragende Balance zwischen Bedienbarkeit und Kompatibilität.

Pro: Benutzerfreundlich; Hauptsitz in Kanada.
Con: Kostenpflichtig.

[1]Dediziert, im engl. dedicated, steht für die Limitierung eines Gerätes auf eine bestimmte Anwendung. Somit bezeichnet „dedizieren“ die Widmung oder Zuweisung einer bestimmten Aufgabe an ein bestimmtes Gerät.

Proton Pass

Proton Pass speichert Daten in der Schweiz so, dass sie durch die strengen Schweizer Datenschutzgesetze geschützt sind.

Pro: Hoher Sicherheitsstandard, Kostenlose Version verfügbar
Con: -

SafeInCloud

Daten liegen lokal auf deinem Gerät oder auf einem Server deiner Wahl, was auch deutsche Server umfassen kann. Du hast die Kontrolle darüber, wo die Daten gespeichert werden.

Pro: Kann selbst konfiguriert werden.
Con: Erfordert gute IT-Kenntnisse; Kostenpflichtig.

Warum ist es interessant, wo der Hersteller seinen Sitz hat?

Jedes Land hat seine eigenen Datenschutzgesetze. In Deutschland gilt die Datenschutzgrundverordnung (DSGVO), die einen weitreichenden Schutz garantiert. In den USA gibt es den „USA Patriot Act“[2], der es US-Behörden wie dem FBI, der NSA oder der CIA den Zugriff ohne richterliche Anordnung auf die Server von US-Unternehmen erlaubt. Auch ausländische Tochterfirmen sind nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren; selbst dann, wenn lokale Gesetze dies untersagen.

Auf Anordnung des FISC, eines Gerichts, dessen Sitzungen und Urteile geheim sind, werden alle Bestands- und Verkehrsdaten von internationalen Nutzern durch die Telefongesellschaften sowie die der US-amerikanischen Internetunternehmen an die NSA übermittelt.

Passwort regelmäßig ändern?

Bis vor kurzem wurde häufig empfohlen, das Passwort regelmäßig zu ändern. Inzwischen raten Datenschutzexperten davon ab - warum sollte man ein sicheres Passwort ändern, wenn es nicht entschlüsselt wurde?

Zudem steigt bei häufigen Änderungen das Risiko, dass der Nutzer sein Passwort vergisst. Oder der Nutzer verliert bei häufigen und aufwändigen Passwortänderungen den Elan und benutzt leichte und kurze Passwörter.

[2] Akronym: **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act** of 2001, deutsch etwa: „Gesetz zur Einigung und Stärkung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu verhindern“.

Allerdings sollte ein Passwort immer dann geändert werden, wenn ein Verdacht auf einen Cyber-Angriff besteht.

Hilfreiche Links:

https://haveibeenpwned.com	taucht meine Mailadresse in einem Datenleck auf?
https://haveibeenpwned.com/passwords/	taucht mein Passwort in einem Datenleck auf?
https://nordpass.com/de/secure-password/	wie sicher ist mein Passwort?

Zusätzliche Sicherheitsebenen

Multi-Factor-Authentication

Aktiviere Multi-Faktor Authentifizierung, wenn es geht. MFA bezieht sich auf die Verwendung von drei oder mehr Faktoren zur Authentifizierung.

- Etwas, das du **weißt** (z.B. ein Passwort oder PIN)
- Etwas, das du **hast** (z.B. ein Smartphone für einen Einmalcode)
- Etwas, das du **bist** (z.B. Biometrie, geographische Position, Verhaltensanalyse)

Beispiel: Neben einem Passwort (etwas, das du weißt) und einem Einmalcode (etwas, das du hast), könnte auch ein biometrischer Faktor wie ein Fingerabdruck (etwas, das du bist) erforderlich sein.

Two-Factor Authentication

Aktiviere die Zwei-Faktor-Authentifizierung, wo es nur geht. 2FA ist eine abgemagerte Form der MFA, bei der zwei Faktoren für die Authentifizierung benutzt werden. Aber dies reicht bereits, um die meisten Bedrohungen abzuwehren.

Beispiel: Du gibst dein Passwort ein (etwas, das du weißt) und erhältst dann einen einmaligen Code auf dein Smartphone (etwas, das du hast). Ohne den Code kannst du dich nicht anmelden.

Passkeys

Passkeys basieren auf öffentlichen und privaten Schlüsseln und ersetzen den Gebrauch von Passwörtern komplett. Das ist eine sicherere Methode[3], denn Passkeys sind nicht anfällig für Phishing-Angriffe oder Passwortdiebstahl. Der private Schlüssel verlässt dein Gerät nie. Stattdessen wird ein Schlüsselpaar verwendet. Der private Schlüssel ist nur auf deinem Gerät gespeichert und der öffentliche Schlüssel auf dem Server.

Jedes Mal, wenn du dich mit deinem Gerät anmeldest, erzeugt dein privater Schlüsselteil im Hintergrund einen neuen, einmaligen Code, der nur mit der Schlüsselhälfte der Webseite oder App entschlüsselt werden kann.

Der Passkey wird automatisch auf deinem Gerät verwendet, was den Prozess viel einfacher und schneller macht.

Passwort gehackt, und nun?

Das Bundesamt für Sicherheit in der Informationstechnik hat einige konkrete Handlungsempfehlungen für den Fall, dass deine Online-Konten kompromittiert wurden:

- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/**Identitaetsdiebstahl**/Hilfe-fuer-Betroffene/hilfe-fuer-betroffene_node.html
- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/**Identitaetsdiebstahl-Social-Media**/identitaetsdiebstahl-social-media_node.html
- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/**Infizierte-Systeme-bereinigen**/infizierte-systeme-bereinigen_node.html

[3] In einem Passkey-basierten 2FA-System könnte der Passkey das traditionelle Passwort ersetzen, während der zweite Faktor (z.B. ein Fingerabdruck oder Einmalcode) das zusätzliche Sicherheitsniveau hinzufügt, das typisch für 2FA ist.
Bei einem MFA-System könnte der Passkey zusammen mit weiteren Faktoren wie einem biometrischen Merkmal (z.. NB. Gesichtserkennung oder Fingerabdruck) und einem Einmalcode auf deinem Smartphone kombiniert werden.