Online-Sicherheit - Sichere Passwörter Co.

Hirschi, Oliver

DOI: https://doi.org/10.36862/eiz-408

Originally published at:
Hirschi, Oliver (2021). Online-Sicherheit - Sichere Passwörter Co. In: Schwarzenegger, Christian; Nägeli, Rolf. Schwachstelle Mensch : Prävention gegen alte und neue Formen der Kriminalität : 12. Zürcher Präventionsforum : Tagungsband 2021. Zürich: Schulthess Verlag, 37-44.
DOI: https://doi.org/10.36862/eiz-408

Online-Sicherheit – Sichere Passwörter & Co.

Oliver Hirschi

Inhalt

I. Einleitung

In der fortschreitenden Digitalisierung werden immer mehr Daten bearbeitet, übertragen und gespeichert, welche geschützt werden müssen. Die Daten liegen auf lokalen Datenträgern oder im Netzwerk und der Cloud. Zum Schutz der Zugänge zu diesen Daten und der Daten selbst, werden vielfach Passwörter eingesetzt.

Die Passwort-Thematik ist ein zweischneidiges Schwert: Auf der einen Seite ein wichtiges Sicherheitselement, auf der anderen Seite ein viel geschasstes Thema aufgrund unzuträglicher Usability. Nichtsdestotrotz sind Passwörter nach wie vor die gängigsten und am meisten verwendeten Schlüssel im digitalen Zeitalter. Sie schützen den Zugriff auf sensible und private Daten.

Die Authentifizierung, beispielsweise bei einem Internetdienstleister erfolgt in der Regel mittels Benutzername oder E-Mail-Adresse und einem Passwort. Das Passwort ist zwar in vielen Fällen nicht mehr das einzige, aber dennoch ein sehr wichtiges Sicherheitselement.

II. Anwendungsbereiche

Passwörter werden primär in zwei Bereichen eingesetzt. Einerseits bei Logins, beispielsweise als Geräteschutz und sehr oft als Zugangsschutz zu Betriebssystemen, Anwendungen und Online-Diensten. In all diesen Fällen erfolgt die Passwortprüfung in der Regel über eine sogenannte Hashfunktion und Hashwert (mehr dazu findet sich im nachfolgenden Kapitel). Andererseits werden Verschlüsselungen (z.B. einzelne Dokumente oder komplette Datenträger) sehr oft mittels Passwörtern geschützt. Hierbei schützt das Passwort entweder direkt den Verschlüsselungsschlüssel oder es dient für die Schlüsselerzeugung.

III. Herausforderungen

Bei der Anwendung von Passwörtern als Sicherheitselement gilt es verschiedenen Herausforderungen zu begegnen, sei es bei der Aufbewahrung/Speicherung, der Übertragung bis hin zur Erzeugung sicherer Passwörter.

1. Hashwerte und Hashfunktionen

Passwörter werden grundsätzlich nicht in Klartext gespeichert, das wäre sehr fahrlässig, sondern als sogenannte *Hashwerte*. Dies, damit niemand ausser dem Benutzer selbst das Passwort kennt – auch der Anbieter/Dienstleister nicht – und das Passwort nicht einfach so gestohlen und missbraucht werden kann.

Hashfunktionen sind sogenannte Einwegfunktionen und dienen dazu einen Text beliebiger Länge (beispielsweise ein Passwort als Input) auf eine „kurze" Zeichenfolge (Hashwert als Output) einer fixen Länge zu transformieren.

Nachfolgende Abbildung zeigt eine vereinfachte Hashfunktion (moderne Hashfunktionen werden in der Regel zusätzlich mit einem sogenannten Salz angereichert, was aber fürs einfachere Verständnis hier vernachlässigt wird).

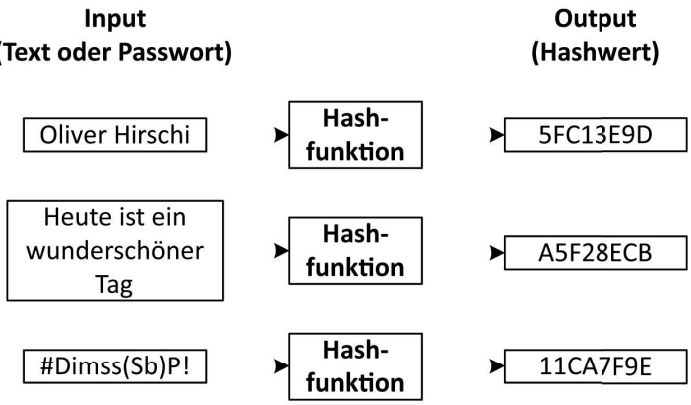

Abbildung 1 – Hashwerte und -funktionen

An Hashwerte und -funktionen werden ganz bestimmte Anforderungen gestellt. Eindeutigkeit, Reversibilität und Kollisionsresistenz stehen dabei im Zentrum:

- **Eindeutigkeit**
  Eine identische Zeichenfolge (Input) soll immer zum selben Hashwert (Output) führen.
- **Reversibilität**
  Der Hashwert (Output) soll nicht in die ursprüngliche Zeichenfolge (Input) zurückberechnet werden können.
- **Kollisionsresistenz**
  Zwei unterschiedliche Zeichenfolgen (Input) sollen nicht den gleichen Hashwert (Output) ergeben.

Sowohl beim Setzen eines Passwortes, als auch beim Authentifizieren wird das eingegebene Passwort durch die Hashfunktion geschleust und entweder abgespeichert (Setzen eines neuen Passwortes) oder mit dem bereits gespeicherten Hashwert überprüft – stimmt dieser überein, hat der Benutzer das korrekte Passwort eingegeben.

2. Angriffe auf Passwörter

Wird die Sicht der Angreifer eingenommen, stellt sich die Frage, wie diese an Passwörter gelangen.

Eine bekannte und sehr weit verbreitete Methode ist das sogenannte *Phishing*, wobei das Passwort beim Opfer direkt „abgefragt" wird (üblicherweise per E-Mail): „Mittels Phishing versuchen Angreifer an Zugangsdaten ahnungsloser Internetbenutzer z.B. zum E-Banking oder zu Online-Shops zu gelangen. Die Täter täuschen dabei eine falsche Identität vor und nutzen so die Gutgläubigkeit ihrer Opfer aus."[1]. Weiter kann ein Angreifer, insbesondere im Mobile-Zeitalter relevant, die Passworteingabe physisch beobachten (sogenanntes *Shoulder Surfing*). Die Abwehrmassnahme dieser beiden Angriffsmethoden ist nicht technischer, sondern menschlicher Natur – das Benutzerverhalten: Der Benutzer ist dafür besorgt, dass er das Passwort nur auf der Website des echten Anbieters eingibt und er dabei nicht beobachtet wird.

Es ist weiter möglich, den Datenverkehr beim Übertragen des Passwortes zum Dienstleister auszuspähen und so das übertragene Passwort mitzulesen (sogenanntes *Sniffing*). Hier hilft als Abwehrmassnahme eine verschlüsselte Datenübertragen mittels TLS/SSL-Protokoll.

Eine weitere, stark verbreitete Methode ist das *Passwort-Hacking*. Dabei werden zuvor beim Dienstleister gestohlene Hashwerte (siehe vorangegangenes Kapitel) gehackt. Brute Force ist dabei nebst weiteren (Wörterbuchangriff und Rainbow Tables hier als Randnotiz) die am weitesten verbreitete Angriffsart.

Beim *Brute Force Angriff* werden alle möglichen Passwort-Kombinationen durchprobiert, bei einem einfachen (enthält nur Zahlen und Kleinbuchstaben) 8-stelligen Passwort z.B. von 00000000 über 9999zzzz bis zzzzzzzz.

Die nachfolgende Tabelle zeigt wie lange es dauert bis ein Passwort mit entsprechender Länge und Komplexität geknackt wird. Als Berechnungsgrundlage wurde eine optimistische (nicht alle Hashfunktionen sind gleich performant), aber für gewisse Hashfunktionen realistische Annahme von 100 Milliarden Versuche pro Sekunde herangezogen.

---

1 <www.ebas.ch/phishing>.

Wie lange dauert es bis ein Passwort gehackt wird?

Anzahl Zeichen	Nur Zahlen 10	Nur Klein- oder nur Grossbuchstaben 26	Zahlen, Gross- und Kleinbuchstaben 62	Zahlen, Gross- und Kleinbuchstaben, Sonderzeichen 95
4	0 Sek.	0 Sek.	0 Sek.	0 Sek.
5	0 Sek.	0 Sek.	0 Sek.	0 Sek.
6	0 Sek.	0 Sek.	1 Sek.	7 Sek.
7	0 Sek.	0 Sek.	35 Sek.	12 Min.
8	0 Sek.	2 Sek.	36 Min.	18 Std.
9	0 Sek.	54 Sek.	38 Std.	73 Tage
10	0 Sek.	24 Min.	97 Tage	19 Jahre
11	1 Sek.	10 Std.	17 Jahre	1804 Jahre
12	10 Sek.	11 Tage	1023 Jahre	171347 Jahre
13	2 Min.	287 Tage	63429 Jahre	16277971 Jahre
14	17 Min.	20 Jahre	3932575 Jahre	1546407714 Jahre
15	3 Std.	532 Jahre	243819668 Jahre	146908685363 Jahre
16	1 Tage	13828 Jahre	15116819415 Jahre	13956325109455 Jahre
17	12 Tage	359534 Jahre	937242803724 Jahre	1325850885398200 Jahre
18	116 Tage	9347891 Jahre	58109053830869 Jahre	125955834112829000 Jahre
19	3 Jahre	243045175 Jahre	3602761337513900 Jahre	11965804240718800000 Jahre
20	32 Jahre	6319174561 Jahre	223371202925862000 Jahre	1136751402868280000000 Jahre

Abbildung 2 – Wie lange dauert es bis ein Passwort mittels Brute Force gehackt ist?

Die Abwehrmassnahme gegen Brute Force Angriffe auf Benutzerseite ist die Verwendung starker Passwörter. Bereits die „19 Jahre“ für ein komplexes 10-stelliges Passwort scheinen sicher genug. Es gilt allerdings zu beachten, dass im Zeitalter des Cloud-Computings verteilte und damit effiziente Berechnungen in der Cloud möglich sind – deshalb die aktuelle Empfehlung der Mindestlänge von zwölf Stellen.

Immer wieder werden Tausende, Millionen Passwort-Hashes gestohlen und anschliessend mittels verschiedener Methoden geknackt (sogenannte Password Breaches). Auf der kostenlosen Website „Have I Been Pwned“ (https://haveibeenpwned.com) sind etliche solche gehackten Passwortlisten hinterlegt und es kann eruiert werden, ob Login-Daten zu einem Online-Konto kompromittiert oder bei einer Datenpanne veröffentlicht wurden.

IV. Sichere Passwörter

Das Hasso-Plattner-Institut (HPI)[2] publiziert jährlich die beliebtesten deutschen Passwörter. Für das Jahr 2020 wurden als Datengrundlage 3.1 Millionen Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers analysiert, welche auf E-Mail-Adressen mit .de-Domäne registriert sind und 2020 geleakt wurden. Auf den Plätzen eins bis fünf der beliebtesten Passwörter stehen „123456“, „123456789“, „passwort“, „hallo123“ und „12345678“.[3] Und auch auf den weiteren Plätzen wird es nicht viel kreativer, sprich sicherer.

2 <https://hpi.de>.

3 <https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html>.

1. Anforderungen

Wie sich ein starkes Passwort zusammensetzt, hat sich im Verlauf der Zeit immer wieder geändert und die Regeln für ein sicheres Passwort wurden jeweils den neusten Gegebenheiten angepasst. Wo vor rund zehn Jahren noch 8-stellige und vor rund fünf Jahren 10-stellige Passwörter als sicher galten, werden heute mindestens zwölf Stellen gefordert. Dies insbesondere aufgrund immer performanteren Technologien, welche zum Hacken von Passwörtern eingesetzt werden.

Verdeutlicht wird dies mit folgendem kleinen Rechenbeispiel: Ein einfaches, 6-stelliges Passwort, welches aus lediglich Kleinbuchstaben und Zahlen besteht ist mit jedem handelsüblichen Notebook innert Minuten knackbar. Für ein komplexes, 12-stelliges Passwort, welches aus Klein-, Grossbuchstaben, Zahlen und Sonderzeichen besteht werden hingegen tausende von Jahren benötigt.

Aus heutiger Sicht gelten nachfolgende sechs Regeln zum sicheren Passwort – verwenden Sie…[4]

- mindestens 12 Zeichen
- Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen
- keine Tastaturfolgen wie z.B. „asdfgh“ oder „45678“
- kein Wort einer bekannten Sprache, d. h. das Passwort sollte keinen Sinn ergeben und in keinem Wörterbuch vorkommen
- überall ein anderes Passwort
- speichern Sie Ihr Passwort nicht unverschlüsselt ab

2. Generierung

Für jeden Dienst unterschiedliche und gleichzeitig starke Passwörter zu verwenden stellt eine Herausforderung dar. Nachfolgende zwei Tipps zum Umgang mit Passwörter helfen dabei: Merksatz und Passwort-Tresor.

Mittels eines *Merksatzes*, den man sich gut merken kann, bildet sich mit den jeweiligen Anfangsbuchstaben sowie Ziffern und Satzzeichen das Passwort:

- „**M**eine **T**ochter **T**amara **M**eier **h**at **a**m **J**anuar **G**eburtstag**!**“
- So entsteht ein starkes Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können:
  „**MTTMha19.JG!**“

[4] <www.ebas.ch/step4>.

Um auch für jeden Dienst ein unterschiedliches Passwort zu verwenden, kann beispielsweise irgendwo im Passwort aus dem Merksatz z.B. die ersten zwei oder drei Buchstaben des Anbieters integriert werden – für den LinkedIn-Zugang entstünde mit obenstehenden Merksatz dann beispielsweise das Passwort „MTTMhaLi19.JG!“.

Mit einem *Passwort-Tresor* (auch Passwort-Manager genannt) können automatisch beliebig lange und starke Passwörter generiert und diese auf sichere Art und Weise (verschlüsselt) gespeichert werden. Ein weiterer Vorteil: Man muss sich lediglich noch ein Passwort merken – das starke Passwort zum Öffnen des Tresors.

V. Erweiterte Authentifizierung

Im Bankenumfeld ist die Multi-/Zwei Faktor Authentifizierung (MFA/2FA) schon längst nicht mehr wegzudenken. Zusätzliche zu einem starken Passwort sorgt sie für noch mehr Sicherheit.

Bei der Multi-/Zwei Faktor Authentifizierung wird zusätzlich zum ersten Sicherheitselement (meistens ein Passwort) ein zweites, unabhängiges Sicherheitselement abgefragt. Mögliche Faktoren sind die drei Bereiche *Wissen* (etwas, das der Benutzer weiss), *Haben* (etwas, das nur der Benutzer besitzt) und *Sein* (etwas, das der Benutzer ist). In der Praxis werden sie beispielsweise wie folgt umgesetzt:

- **Wissen**
  Passwort, PIN, Sicherheitsfrage, …
- **Haben**
  Chip-Karte, Schlüssel, Mobiltelefon, Zertifikat, …
- **Sein**
  Fingerabdruck, Gesichtserkennung, Spracherkennung, …

Mittlerweile bieten nebst Banken auch viele weitere Online-Dienstleister (z.B. Google, Facebook) eine Zwei-Faktor-Authentifizierung an.

VI. Ausblick

Wie sieht die Zukunft der Passwörter als Sicherheitselement aus? Hoffentlich nicht 14-, 16- oder gar 18-stellige Passwörter. Die Herausforderung einer sicheren und benutzerfreundlichen Authentifizierung ist gross. Es gibt verschiedene Bestrebungen, Passwörter überflüssig zu machen, allerdings ist *die* Lö-

sung noch nicht gefunden. Der FIDO2 Standard der FIDO Alliance[5] hat sich (noch) nicht durchgesetzt, vielleicht könnte auch das allgegenwärtige Smartphone und/oder die Mobile-Nummer genutzt werden, oder etwas ganz anderes/neues.

Bis dahin gilt es starke Passwörter zu erstellen, verwenden und verwalten, um die Zugänge und Daten bestmöglich zu schützen.

[5] <https://fidoalliance.org>.