Pa$w0rter?

Warum die Forderung nach Sonderzeichen in Passwörtern die Sicherheit nicht unbedingt erhöht.

| von DR. ROGER FISCHLIN

Passwörter dienen beim Zugriff auf Computersysteme seit jeher zur Authentifizierung des Nutzers, also zum Nachweis von dessen Identität. Passwörter müssen sicher sein, denn wer die Anmeldedaten eines Nutzers kennt, kann sich im System auch als Nutzer ausgeben. Deshalb verlangen Sicherheitsstandards sowie Richtlinien in nahezu jeder Organisation komplexe Passwörter, die zudem regelmäßig geändert werden müssen. Diese Anforderungen stammen aus dem NIST-Standard „Special Publication SP 800-63“ von 2003. Einer der damaligen Autoren, Bill Burr, räumt heute mit Blick auf die Regeln allerdings ein, er bereue vieles von dem, was er getan habe. Doch warum? Wie hat sich die Sicht auf Passwörter und auf die Risiken in den letzten Jahren geändert? Was empfiehlt die amerikanische Bundesbehörde National Institute of Standards and Technology (NIST) in der neuen Fassung des damals richtungsweisenden Standards SP 800-63?

ANGRIFFE AUF PASSWÖRTER

Im Kern basiert jeder Diebstahl eines geheimen Passworts auf Raten. Die Knobelei lässt sich technisch zwar nicht vollständig verhindern, aber man kann die Erfolgswahrscheinlichkeit senken beziehungsweise den Aufwand erhöhen, sodass ein Passwortdiebstahl nicht mehr praktikabel wird. Es gibt zwei Grundtypen von Angriffen:

- Online: Der Angreifer prüft mögliche Passwörter, indem er sie direkt beim Zielsystem ausprobiert.
- Offline: Der Angreifer prüft mögliche Passwörter, indem er sie mit Passwortinformation des Zielsystems abgleicht, die er sich zuvor irgendwie besorgt hat.

Die meisten Systeme wirken Onlineangriffen effektiv entgegen: Sie verzögern nach aufeinanderfolgenden Fehlversuchen zunächst weitere Anmeldeversuche (Throttling), um den zeitlichen Aufwand zu erhöhen, bevor sie bei fortgesetzten Rateversuchen den Zugang bis zur Klärung komplett sperren.

Bei einem Offlineangriff verfügt der Angreifer über Passwortinformationen aus einem Datenleck, etwa aus einem digitalen Einbruch (Breach) oder von einer internen Quelle, die die Zugangsdaten bewusst oder fahrlässig weitergegeben hat (Data Leakage). Sollten die Passwörter im Klartext vorliegen, ist der Angriff trivial. Daher speichern moderne Systeme keine Passwörter, sondern nur deren Hashwerte. Eine kryptografische Hashfunktion liefert zu verschiedenen Passwörtern verschiedene Hashwerte fester Bitlänge, ohne dass man aus den Werten die Eingaben rekonstruieren kann (Oneway-Eigenschaft). Bei einer Anmeldung berechnet das System den Hashwert des Passworts und vergleicht ihn mit dem hinterlegten Wert.

Die Kenntnis des Hashwerts ohne Passwort reicht nicht aus, um sich anzumelden. Der Betrüger versucht beim Offlineangriff, zu vorliegenden Hashwerten passende Anmeldedaten zu finden. Das Brute-Force-Vorgehen, bei dem man im trivialsten Fall alle Möglichkeiten ausprobiert, ist in der Regel zu aufwendig. Hacker verwenden lieber Datenbanken (Wörterbücher beziehungsweise allgemeine Sammlungen gestohlener beziehungsweise regelmäßig eingesetzter Passwörter), gepaart mit Regeln für gängige Modifikationen wie Buchstaben durch ähnlich aussehende Ziffern oder Sonderzeichen auszutauschen.

Das Zielsystem ist bei dem Abgleich nicht involviert, kann den Offlineangriff also nicht aktiv stoppen. Als Gegenmaßnahme zwingt es Nutzer, ihre Passwörter regelmäßig zu ändern, bevor es rechnerisch durch einen Angreifer erraten wird. Als weitere Maßnahme sind die üblichen Passwort-Hashverfahren so konstruiert, dass sie Zeit in Anspruch nehmen – ein einzelner Wert lässt sich zwar ohne relevante Verzögerung bestimmen, die Berechnung sehr vieler Hashwerte ist indes zeitintensiv und stößt schnell an ihre Grenzen. Allerdings lässt sich die Arbeit parallelisieren, außerdem gibt es fertige Tabellen mit üblichen Passwörtern und zugehörigen Hashwerten. Um Anmeldedaten zu erraten, genügt dann ein Blick in die Tabelle. Doch es gibt eine gängige Gegenmaßnahme: Systeme ergänzen Passwörter um eine zufällige Folge und wenden dann das Hashverfahren an. Dann erhöht das hinzugefügte sogenannte Salt (Salz) den Grad der Zufälligkeit in der Zeichenfolge (Entropie). Selbst wenn der zufällige Salt öffentlich wird, sind die vorhandenen Tabellen nutzlos.

ALTE ANFORDERUNGEN AN PASSWORTE UND DIE PRAXIS

Die übliche Maßnahme gegen Raten ist ein hinreichend komplexes Passwort. Um die Komplexität zu messen, hat das NIST in der alten Version ihres Standards eine Passwortentropie, angelehnt an Shannons Informationstheorie, formuliert. Vereinfacht ausgedrückt: Je höher der Wert, desto zufälliger ist die Zeichenfolge und desto schwieriger sollte ein Angreifer die Anmeldedaten erraten können. Auf diesem Ansatz fußen die Anforderungen, die nahezu in allen Sicherheitsstandards und Richtlinien auch heute noch zu finden sind:

- Mindestens acht druckbare Zeichen
- Mindestens ein Groß- sowie ein Kleinbuchstabe, eine Ziffer und ein Sonderzeichen
- Kein geläufiges Wort aus einem Wörterbuch
- Nicht der Log-in-Name

Um Offlineangriffe ins Leere laufen zu lassen, sollten Nutzer ihre Passwörter spätestens alle 90 Tage ändern.

Es ist eine Ironie, dass von Hackern im letzten Jahrzehnt gestohlene und aus verschiedenen Motiven anschließend veröffentlichte Passwortsammlungen zur Stärkung der Sicherheit beigetragen haben. Denn die große verfügbare Datenmenge zeigt, welche Passwörter Menschen wählen und wie sie die gängigen Regeln umsetzen. Solche Informationen standen den Autoren des NIST-Standards vor 15 Jahren noch nicht zur Verfügung. Weir et al.[1] haben die Passwortentropie in Experimenten mit realen Passwortsammlungen untersucht und kommen zu dem Schluss, das Konzept sei kein valides Maß für die Sicherheit eines Passworts gegen Raten. In seiner Dissertation[2] hat Weir die Häufigkeit der Zeichen anhand gehackter Anmeldedaten aus veröffentlichten Sammlungen untersucht:

- Das letzte Zeichen ist sehr häufig eine Ziffer, oft die Eins.
- Kleinbuchstaben sind viel häufiger als Großbuchstaben.
- Sonderzeichen sind selten, am meisten werden Ausrufezeichen und Punkt genutzt.

Auch die gerne in Zeitschriften publizierten Rankings der beliebtesten Passwörter offenbaren ein düsteres Bild hinsichtlich Kreativität der Nutzer und Qualität der Anmeldedaten. In der Praxis führen die Regeln nicht dazu, dass Nutzer das gesamte Universum bei der Wahl ihres Passworts gebrauchen. Sie berücksichtigen vielmehr akribisch die Mindestansprüche, so sind etwa Anmeldedaten mit mehr als acht Zeichen selten. Für die Mehrheit der Passwörter gilt: Anforderung erfüllt, Ziel verfehlt. Jim Fenton, einer der Verfasser der neuen SP 800-63, formuliert es frei übersetzt so: „Wen Vorgaben stören, der mogelt sich irgendwie durch“.[3] Weist ein System beispielsweise ein Passwort als zu schwach oder kurz ab, machen viele simple Modifikationen, wie eine Eins oder ein Ausrufezeichen anhängen, bis die Eingabe akzeptiert wird. Wer alle paar Wochen sein Passwort ändern muss, greift oft auf Hochzählpasswörter zurück: Man ergänzt einfach einen Zähler am Ende des Passworts, wodurch faktisch sogar kürzere Passwörter akzeptiert werden. Der Mensch will und kann sich nicht ständig neue komplexe Passwörter merken. Die Regel fördert auch die gängige und doch sehr gefährliche Praxis, bei mehreren Systemen die gleichen Anmeldedaten (Log-in und Passwort) zu nutzen. Das am wenigsten geschützte System gibt die Sicherheit des Passworts auf allen Systemen vor, und ist das Passwort einmal bekannt, ist der Identitätsdiebstahl kaum noch zu verhindern.

Passwortdiebe wissen leider um die menschlichen Schwächen und können so für ihre Angriffe den Suchraum deutlich einschränken. Betrüger finden bei einem Offlineangriff schwache Passwörter heute schneller, als Benutzer sie ändern. Das NIST spricht von mehreren Milliarden Passworten, die moderne Rechner mit ausgeklügelten Algorithmen wie Rainbow-Tables pro Sekunde testen können.[4] Auch kryptische Passwörter helfen per se nicht, denn ein Computer kennt keine Sprachen – für ihn sind alles Zeichenfolgen, die er bis zu einer gewissen Länge einfach durchprobiert. Der Mensch beherrscht Sprachen, für ihn hat eine scheinbar wirre Zeichenfolge keinen Sinn, weshalb er sie sich kaum merken kann. Menschen notieren sich solche Informationen als Gedächtnisstütze, bunte Klebezettel am Monitor und

WURDE MEIN PASSWORT SCHON GEHACKT?

Auf folgenden Seiten kann man prüfen, ob seine E-Mail-Adressen von bekannten Datenabflüssen betroffen sind:

- https://sec.hpi.de/ilc/
- https://haveibeenpwned.com/
- https://monitor.firefox.com/
- https://breachalarm.com/

Fällt die Suche positiv aus, sollte man das Passwort in allen Systemen, in denen man es nutzt, unverzüglich ändern.

Der bekannteste Dienst aus Deutschland ist der „Identity Leak Checker" (ILC) vom Hasso-Plattner-Institut. Die Webseite www.haveibeenpwned.com des Australiers Troy Hunt umfasst derzeit rund 7,8 Milliarden Einträge. Der Begriff „pwnd" stammt aus der Gaming-Szene (als Tippfehler von „owned") und bedeutet übersetzt etwa: „Ich hab' dich!". Die Seite bietet auch die Möglichkeit, statt nach E-Mail-Adressen nach Passwörtern im Datenbestand zu suchen.

Da man Passwörter nicht an Dritte geben sollte, wird nur der lokal im Browser berechnete Hashwert übertragen. Nichtsdestotrotz besteht ein Restrisiko, dass Dritte das Passwort erfahren, auch wenn die Webseite als seriös gilt. Hinter jedem Test, ob das eigene Passwort gehackt wurde, kann die Phishing-Webseite eines Betrügers stecken. Daher sollte man grundsätzlich nie sein Passwort auf anderen Webseiten eingeben, speziell nicht, wenn man über eine E-Mail-Nachricht dazu unter Druck aufgefordert wird.

Zettel unter der Tastatur erfreuen sich großer Beliebtheit. Warum eigentlich die Anfangsbuchstaben der Wörter eines Satzes als Passwort wählen, wenn man den Satz selber nehmen kann? Jim Fenton folgert, man möge Nutzer nicht zu Sachen zwingen, die die Sicherheit nur unwesentlich stärken. Menschliches Verhalten verkehrt die Absicht zudem schnell ins Gegenteil, viele Regeln sind in der Praxis kontraproduktiv für die Sicherheit.

NEUE ANFORDERUNGEN AN PASSWÖRTER

Nutzer empfinden die üblichen Passwortregeln häufig verständnislos als Gängelung und versuchen, sich mit minimalem Aufwand und so vorhersehbarem Verhalten durchzumogeln. Bill Burr glaubt, die Regeln damals waren zu kompliziert, als dass die meisten ihren Sinn verstanden haben. In Wirklichkeit, so fährt er resigniert fort, habe man im Ergebnis mit den Regeln den falschen Baum angebellt.[5] Das NIST zieht in der aktuellen Fassung nüchtern das Fazit: Es habe sich gezeigt, dass die Länge der wichtigste Faktor für Sicherheit sei.

Daher fordert die amerikanische Behörde in der neuen Fassung des Standards SP 800-63 für die von Nutzern gewählten Passwörter:

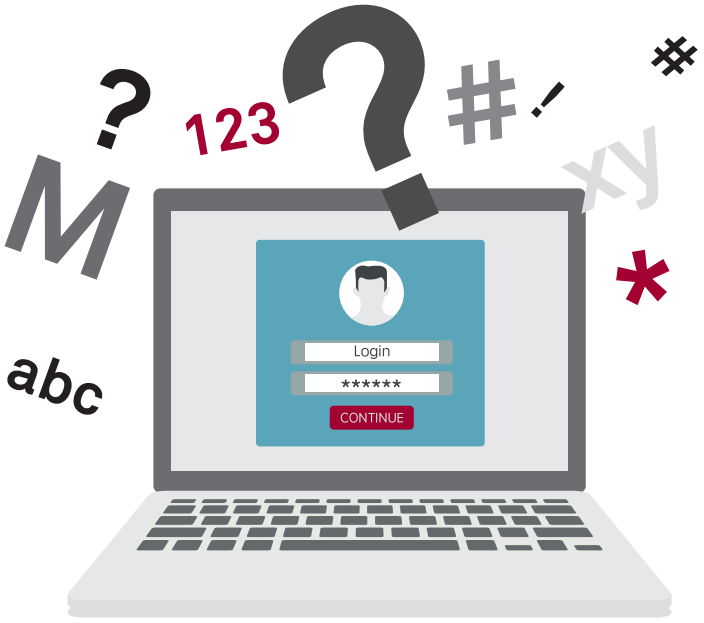
- Mindestens acht Zeichen inklusive Leerzeichen.
- Nicht auf der Liste ungeeigneter Passwörter für das System.

Die acht Zeichen stellen die Minimalforderung dar, da kürzere, auch zufällige generierte Passwörter in jedem Fall unsicher sind. Das System soll grundsätzlich Passwörter mit mindestens 64 Zeichen akzeptieren, sodass Nutzer sich leicht zu merkende ganze Sätze wählen können. Die Länge soll nur durch technische Randbedingungen begrenzt werden, das Passwort darf nicht nach einer bestimmten Position vom System abgeschnitten werden. Man kommt dem Nutzer dahin gehend entgegen, dass künftig auch Leerzeichen erlaubt sind. Das NIST macht ausdrücklich keine Vorgaben für die einzelnen Zeichen. Da Passwörter heute nicht mehr im Klartext in einer Datenbank gespeichert werden, ist die Furcht vor SQL-Injection-Angriffen durch Leer- oder Sonderzeichen in Passworten unbegründet. Als Hashfunktion soll ein nach Standard zugelassenes Verfahren verwendet werden, um den Schutz gegen Offline-Angriffe durch eine unpassende Wahl nicht zu schwächen. Bei der Anmeldung soll der Nutzer gemäß NIST-Standard die Möglichkeit haben, sich die Eingabe anzeigen zu lassen oder zumindest kurz das jeweils letzte Zeichen. Nutzer sollen Passwörter in die Eingabemaske kopieren dürfen, um so Passwortmanager zu unterstützen, denn aus Sicht der Fachleute erhöhen diese Werkzeuge in den meisten Fällen die Wahrscheinlichkeit, dass Nutzer sichere Passwörter nutzen.

Auf der Liste ungeeigneter Passwörter sollen solche stehen, von denen bekannt ist, dass sie allgemein verwendet werden, vorhersagbar oder bereits kompromittiert sind. Das NIST gibt keine Liste vor, sondern nennt als nichtabschließende Aufzählung:

- verfügbare Sammlungen gehackter Passwörter,
- Wörterbücher,
- wiederholte oder fortlaufende Zeichen (wie „aaaaaa" oder „123456"),
- kontextspezifische Wörter wie der Name des Dienstes, Nutzername usw. sowie Varianten davon.

Das System soll Nutzern erklären, warum es ein Passwort als unsicher ablehnt, und Verbesserungsvorschläge geben, um trivialen Modifikationen vorzubeugen. Antworten auf vorgegebene



Fragen, etwa die beliebten Sicherheitsabfragen nach dem Geburtsort oder Namen des Haustiers, sind zur Identifikation ungeeignet, da sie in der Regel leicht zu erraten sind.

Das Hochzählen des Passworts kann nach Ansicht des NIST ein Ende haben. Nutzer sollen künftig nicht mehr gezwungen werden, ihre Passwörter regelmäßig zu ändern – es hat sich in der Praxis als nicht förderlich für die Sicherheit herausgestellt. Nur bei Hinweisen auf Kompromittierung soll das System Nutzer auffordern, ein neues Passwort zu wählen. Denn Offlineangriffe basieren heute auf Wörterbüchern und Listen, nicht auf dem stupiden Ausprobieren aller Passwörter im Wettlauf gegen die Zeit. Gegen dieses reale Bedrohungsmodell (Threat Model) liefert der neue Ansatz für die Passwortwahl einen besseren Schutz als das regelmäßige Ändern des Passworts.

AUSBLICK

Der populäre Sicherheitsexperte Bruce Schneier schreibt in seiner Kolumne, man müsse dem Nutzer aus dessen Sicht widersinnige Dinge auferlegen, weil das Sicherheitsdesign oft einfach schlecht sei.[6] Man möge, so der Appell des Experten, nicht versuchen, die Defizite auf Ebene des Nutzers zu beheben. Als Beispiel nennt er explizit Passwörter.

Die Authentifizierung über Passwörter wird es auch in Zukunft geben, sie ist einfach und erfordert keine zusätzliche Hardware. Perfekte Sicherheit können anderen Methoden wie Fingerabdruckscanner nicht gewährleisten, Hacker zeigen immer wieder medienwirksam Schwachstellen auf. Passwortmanager bieten oft Generatoren, die zufällige Passwörter erzeugen, die zwar sicher sind, man sich aber die kryptischen Zeichenfolgen nicht merken kann. Die Verfügbarkeit und Sicherheit aller Zugangsdaten hängt dann vom Passwortmanager ab; möchte der Nutzer sich von mehreren Geräten anmelden, müssen die (verschlüsselten) Daten in der Cloud liegen. Der Zugang zum Passwortmanager erfordert eine Authentifizierung des Nutzers, meist über ein Passwort.

NIST folgend hat das Britische National Cyber Security Centre (NSSC) seine Regeln für Passwörter ebenfalls an die Erkenntnisse des menschlichen Verhaltens ausgerichtet.[7] Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt auf seinen Seiten ähnliche Hinweise zur Passwortsicherheit.[8] Indes, in ihrem Grundschutz hält die Sicherheitsbehörde noch an der alten Lehre fest und fordert nach ORP.4.A8 Passwörter mit ausreichender Länge und Komplexität, die in angemessenen Zeitabständen geändert werden sollten.[9] Auch in Richtlinien vieler Organisationen finden sich heute noch die alten Ansätze.

Die an die Erkenntnisse im Umgang mit Passwörtern angepassten Regeln lösen allerdings die grundsätzlichen Schwächen einer passwortbasierten Authentifizierung nicht. So schützt auch das beste Passwort nicht gegen Phishing-Angriffe oder Keylogger. Wer hohe Sicherheit will, der sollte über eine Mehr-Faktor-Authentifizierung nachdenken anstatt über verschärfte Passwortregeln. ●

1 Weir, M.; Aggarwal, S.; Collins M.; Stern, H.: „Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords", ACM CCS '10, 2010.
2 Weir, M.: „Using Probabilistic Techniques to Aid in Password Cracking Attacks", Dissertation, Florida State University, 2010.
3 Fenton, J.: „Toward Better Password Requirements", online verfügbar unter https://www.slideshare.net/jim_fenton/toward-better-password-requirements (abgerufen am 16.11.2018).
4 NIST: „NIST Special Publication 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management", 2017.
5 McMillan, R. : „Password Rules Expert Has A New Tip: N3v$rM1nd! ", Wallstreet Journal, 2017. Online verfügbar unter https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118 (abgerufen am 16.11.2018).
6 Schneier, B.: „Stop Trying to Fix the User", IEEE Security & Privacy, Band Volume: 14, Heft 5, 2016. Online verfügbar unter https://ieeexplore.ieee.org/document/7676198 (abgerufen am 16.11.2018).
7 UK National Cyber Security Centre (NCSC): „Password Guidance: Simplifying Your Approach", 2016. online verfügbar unter https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach (abgerufen am 16.11.2018).
8 Bundesamt für Sicherheit in der Informationstechnik: „Grundschutzkompendium", Baustein ORP.4 Identitäts- und Berechtigungsmanagement. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html (abgerufen am 16.11.2018).
9 Bundesamt für Sicherheit in der Informationstechnik: „Grundschutzkompendium", Baustein ORP.4 Identitäts- und Berechtigungsmanagement. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html (abgerufen am 16.11.2018).