esatus AG
Enforcing Information Security

Passwort neu gedacht: Definition einer modernen Password Policy

Die prägende Situation im Spielfilm „The Truman Show“, bei der Truman Burbank nach einem Lebensabschnitt unter völliger Kontrolle und Überwachung seinem Schöpfer mit den Worten „You never had a camera inside my head.“ entgegentritt, verdeutlicht, wo unsere geheimsten Informationen nach wie vor am besten geschützt sind: In unserem Kopf.
Etablierte Password Policies im geschäftlichen Umfeld basieren zumeist auf den veralteten Regeln einer Publikation des NIST (*NIST Special Publication 800-63, appendix A [1]*) aus dem Jahre 2003 und führen nicht selten dazu, dass diese nicht mehr im Kopf, sondern im besten Falle in elektronischen Password Safes und im schlechtesten Falle auf einem Zettel unter der Tastatur landen. Wie kann eine moderne Password Policy es schaffen, für mehr Sicherheit und zugleich Benutzerakzeptanz zu sorgen?

Sebastian Weidenbach
Head of Technical Consulting & Solutions, CISSP

Einleitung

William E. Burr hatte während seiner Arbeit an der Electronic Authentication Guideline für das National Institute of Standards and Technology nicht ahnen können, dass seine Arbeit nicht zum gewünschten Ziel führen würde. Von ihm stammen die bekannten Passwortkriterien:

- Mindestens eine Ziffer
- Mindestens ein Sonderzeichen
- Regelmäßige Erneuerung des Passworts

Nun, 14 Jahre später, nachdem sein Regelwerk internationale Anwendung gefunden hat, zeigt er sich gegenüber dem Wall Street Journal [2] einsichtig und sagt:

„It just drives people bananas and they don't pick good passwords no matter what you do.“

Dabei hatte er insbesondere die Kreativität der Benutzer unterschätzt. Je komplexer das Passwort und je häufiger die erzwungene Erneuerung, desto wahrscheinlicher ist es, dass das Passwort z. B. durch die massenhafte Verwendung von Monat und Jahreszahl zwar den Richtlinien genügt, aber zukünftige Passwörter berechenbar werden und sich von Benutzer zu Benutzer nicht sonderlich unterscheiden. Dazu kommt, dass Benutzer dazu neigen, sich das Passwort aufzuschreiben oder digital abzulegen.
Moderne Passwortfilter können Blacklists verwenden, um Passwörter mit unerlaubten Bestandteilen zu verbieten und beachten darüber hinaus die Passworthistorie, um zu ähnliche Passwörter zu erkennen. Jedoch sind sie derzeit nicht in der Lage, der Kreativität der Benutzer etwas entgegenzusetzen und effektiv vor unsicheren Passwörtern zu schützen.
Speichert ein Benutzer sein Passwort in digitaler Form, so sind weitere Risiken damit verbunden:

- Abgriff des Passworts bei unsicherer Übertragung über das Netzwerk
- Nutzung eines Password Safes aus nicht vertrauenswürdiger Quelle oder mit nicht vertrauenswürdiger Ablagetechnologie

Ein Umdenken im Umgang mit Kennwortrichtlinien erscheint sinnvoll und wird im Folgenden näher betrachtet. Insbesondere die rechtlichen und regulatorischen Konsequenzen werden dabei im Detail beleuchtet.

Identitätsdiebstahl

Sichere Passwörter schützen die Vertraulichkeit von Informationen und sorgen für Authentizität im kollaborativen Umgang mit Daten.
Wird ein Passwort gestohlen, so kann die von ihm geschützte Identität von Angreifern verwendet werden.

Typische Szenarien zur Erlangung eines Passworts sind:

- Mitschneiden der Tastatureingabe durch einen **Keylogger**
- Automatisches „Erraten" des Passworts (**Bruteforce** Angriff)
- Erkennung üblicher Passwörter durch Nutzung eines digitalen Wörterbuchs (**Dictionary attack**)
- **Social Engineering** (z. B. Preisgabe des Passworts durch gefälschte Anweisungen zum Zurücksetzen des Passworts per Phishing E-Mail)
- Ausspähen von Passwörtern, z. B. unter der Tastatur, aber auch auf alten Festplatten und im Papierkorb (**Information diving**)

Hat der Identitätsdiebstahl stattgefunden, so können die Folgen fatal sein. Der Verlust von geschäftskritischen Informationen kann schwere finanzielle und reputative Schäden hervorrufen, die nicht selten die Existenz einer Organisation oder eines Unternehmens bedrohen.

Was tun?

Wie erörtert, führen die Erhöhung der Komplexität und die Verringerung der Passwortgültigkeit nicht unmittelbar zu einer Verbesserung der Sicherheit. Es bleibt die Frage, was ein sicheres Passwort ausmacht und wie man den Nutzer dazu bewegt, ein solches Passwort festzulegen.

Es existieren eine Vielzahl von alternativen Authentifizierungsmethoden, die je nach Kritikalität der zu schützenden Informationen und der Bereitschaft höhere Kosten in Kauf zu nehmen, die richtige Wahl sein können:

- Biometrische Authentifizierung
- Smartcard Authentifizierung
- Software und Hardware Tokens
- Digitale Zertifikate
- Kombination mehrerer Authentifizierungsfaktoren (2FA)

Diese Methoden werden, genauso wie die Ausstellung eines generierten Passworts, im Folgenden nicht eingehender diskutiert, sondern stattdessen Möglichkeiten der Modernisierung von benutzerdefinierten Passwörtern fokussiert.

Ein Beispiel einer modernen Password Policy könnte wie folgt aussehen:

- Keine Komplexitätsvorgaben
- Passwortlänge flexibel zwischen 20 und 64 Zeichen
- Prüfung und Ausschluss bekannter Passphrasen
- Kein erzwungenes Ablaufdatum

Ein valides Passwort wäre demnach „Ich-bin1982inFrankfurtzurSchulegegangen".

Förderlich ist zudem, alle druckbaren Zeichen des UTF-8 Zeichensatzes zu akzeptieren, um die Kreativität der Nutzer nicht unnötig einzuschränken.

Durch den Verzicht auf Komplexitätsvorgaben kann sich der Benutzer für Passphrasen, also zum Beispiel zusammenhängende Sätze, entscheiden. Diese sind einprägsamer und es sinkt der Bedarf zur Ablage des Passworts. Da das Passwort nicht abläuft, wird dieser Effekt noch verstärkt.

Wichtig ist zudem die Etablierung eines Security Awareness Programms im Unternehmen, um den Umgang mit Passwörtern zu erläutern und bei der Wahl des Passworts zu helfen.

Die Länge des Passworts wirkt – trotz geringerer Komplexität – der Möglichkeit entgegen, dass das Passwort per Bruteforce Attacke erraten wird.

Der verlorene Schutz durch regelmäßige Passworterneuerung muss jedoch genauer betrachtet werden.

Muss ein Passwort beispielsweise alle vier Wochen erneuert werden, so kann ein gestohlenes Passwort über diesen Zeitraum hinaus nicht genutzt werden. Jedoch hat der Angreifer, je nach Zeitpunkt des Abgriffs, zumeist genügend Möglichkeiten, um mit den gestohlenen Zugangsdaten z. B. ein Backdoor per Schadprogramm auf dem PC des Opfers zu platzieren. Mit diesem sind zukünftige Zugriffe auch ohne Passwort möglich, wodurch der Mehrwehrt in Frage zu stellen ist.

Viel wichtiger ist, dass ein unerlaubter Zugriff durch detektive Kontrollmaßnahmen (z. B. durch Intrusion Detection Systeme) erkannt wird. In diesem Falle und auch wenn der Benutzer selbst mit einem Abgriff seines Passwortes rechnen muss, sollte eine Passworterneuerung ereignisgetrieben eingeleitet werden. Bezogen auf die Angriffsmöglichkeiten ergibt sich daraus eine deutliche Verbesserung:

	Klassische PW Policy	Moderne PW Policy
Keylogger	⊖	⊖
Bruteforce	⊕	⊕
Dictionary attack	⊖	⊕
Social Engineering	-	-
Information diving	⊖	⊕

Tabelle 1 - Gegenüberstellung der Password Policies

Regulatorik

Besonders in regulierten Branchen ist ein primäres Ziel, die Informationssicherheit konform zu gültigen Standards und Rechtsvorgaben zu halten. Da die restriktiveren Passwortrichtlinien aus der veralteten NIST Publikation in zahlreicher Form adaptiert wurden, ist die Verwendbarkeit einer überdachten Password Policy nicht immer gewährleistet und muss im Einzelfall evaluiert werden.

Dabei ist zunächst festzustellen, dass auch die NIST SP 800-63-3B zwischenzeitlich (2016) erneuert wurde und einen moderneren Umgang mit Passwörtern beschreibt. Speziell im BSI Grundschutz M 2.11 (Stand 2016) werden einige SOLL-Eigenschaften beschrieben, die zu beachten sind. So wird grundsätzlich ein Passwort gefordert, welches leicht zu merken ist, jedoch aus mindestens zwei Zeichenarten (Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen) besteht. Hinzu kommt als MUSS-Eigenschaft, dass das Passwort regelmäßig (z. B. alle 90 Tage) gewechselt wird. Somit ist das genannte Beispiel einer modernen Password Policy mit dem aktuellen Stand des BSI Grundschutz nicht vereinbar. Die gleichen Schwierigkeiten gibt es mit den PCI DSS [3] (Anforderungen 8.2.3 und 8.2.4) in Version 3.2 (Stand April 2016).

Anders verhält es sich mit der ISO 27002 [4] aus dem Jahr 2017. Hier wird in den Controls 9.3.1 und 9.4.3 der Einsatz von „starken" Kennwörtern gefordert. Kerneigenschaften sind dabei die Einprägsamkeit und dass es nicht durch Dictionary attacks angreifbar ist, was mit dem aufgezeigten Beispiel vereinbar scheint.

Grundsätzlich scheint dies auch für die in der DSGVO [5] in Art. 32 (Sicherheit der Verarbeitung) beschriebenen Pflicht zur Sicherstellung eines angemessenen Schutzniveaus (abhängig von Zweck und Umfang der gespeicherten Daten) zuzutreffen. Hierbei muss beachtet werden, dass der jeweilige Stand der Technik Beachtung findet und die Auslegung in der Praxis derzeit nur schwer absehbar ist. In jedem Falle empfiehlt sich eine risikobasierte Entscheidungsfindung, um ein angemessenes Handeln im Sinne der Anforderungen nachweisen zu können.

Fazit

Die Passwortauthentifizierung ist für viele IT-Systeme dominierend. Wenn keine fortschrittlicheren Verfahren, wie die Mehrfaktorauthentifizierung, zur Verfügung stehen oder die Integrations- und Betriebskosten solcher Lösungen nicht verhältnismäßig sind, sollte die Auswahl der Passwortkriterien sorgfältig überlegt sein. Sicherheit und Benutzerakzeptanz führen in Richtung längerer Passwörter, die aber leichter zu merken sein müssen. Weitere Faktoren, abhängig von Unternehmensgröße und Branche, spielen ebenso eine große Rolle, sodass eine geeignete Policy immer aus einer individuellen und risikobasierten Betrachtung hervorgehen sollte.

[1] NIST Special Publication 800-63B, Juni 2017 https://doi.org/10.6028/NIST.SP.800-63b

[2] The Wall Street Journal – "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!", 07.08.2017 https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

[3] Payment Card Industry Data Security Standard, Version 3.2 - 2016

[4] DIN EN ISO/IEC 27002:2017, Juni 2017

[5] Datenschutz Grundverordnung (DSGVO 2016/679)

Herausgeber **esatus** AG

Grafik Seite 1 © Fotolia / Tomasz Zajda

Stand der Informationen: Januar 2018