Die Passwort-Falle: Wenn der Mensch zum Risikofaktor wird

6 November 2019 | **Cyber Security** | **Raphael Reischuk**
Lesezeit: 9 Minutes

Über 80% aller Cyber-Angriffe werden über menschliche Schwachstellen gestartet. Mangelndes Bewusstsein und fehlende Sachkenntnisse der Mitarbeitenden – kombiniert mit der zunehmenden digitalen Vernetzung – machen es Cyber-Kriminellen leichter denn je zuvor, sich in fremden Unternehmensstrukturen einzunisten, Daten abzuführen und ganze Systeme lahmzulegen. Für Firmen endet dies oft mit Verlusten in Milliardenhöhe. Um sich wirkungsvoll gegen Hacker-Angriffe zu schützen, braucht es eine allumfassende Sicherheitsstrategie, die möglichst viele Risiken berücksichtigt. Angefangen bei den Mitarbeitenden.

Die Frage ist heute nicht mehr, ob, sondern wann eine Cyber-Attacke stattfindet. Unternehmen müssen sich heute damit auseinandersetzen, wie die Gefahren frühzeitig erkannt werden können und Angriffen mit Widerstandskraft begegnet werden kann. Neben technischen Massnahmen und Prozessanpassungen, sind die Mitarbeitenden der Schlüsselfaktor in der Abwehrstrategie. Sind diese nicht oder zu wenig auf das Thema sensibilisiert, werden sie zum ersten und einfachsten Einfallstor für gezielte und hochspezialisierte Angriffe auf das Unternehmen. In einer ganzheitlichen Security-Strategie sind intensive Aufklärungs- und Ausbildungsarbeit der Mitarbeitenden also zwingender Bestandteil.

Eine effektive Massnahme, um die Informationssicherheit im Unternehmen durch die Belegschaft zu stärken, führt über den simplen Weg von raffinierten Passwörtern. Denn die grösste Angriffsfläche, die durch den Menschen verursacht wird, entsteht – neben Phishing-Mails und Social Engineering – durch die wiederholte Verwendung von Kennwörtern. Zwar sprechen viele Experten seit Jahren von der Abschaffung von Passwörtern, doch erfreuen sie sich nach wie vor grosser Beliebtheit bei Entwicklern und Anwendern: für jedermann verständlich, vergleichsweise einfach zu implementieren, portabel und jederzeit austauschbar. Gehen wir also mal davon aus, dass Passwörter nicht so schnell abgelöst werden.

Dieser Beitrag stellt eine Möglichkeit vor, sich unbegrenzt viele, und dennoch eindeutige und zugleich komplexe Passwörter im Kopf zu merken. Hier geht´s zur Videoserie:

Part I: Authentifizierung
Part II: Die Essenz eines guten Passworts

Part III: Schritt für Schritt zum sicheren Passwort

Der Reihe nach: Warum dürfen Passwörter auf keinen Fall wiederverwendet werden?

Wird ein und dasselbe Passwort auf verschiedenen Plattformen oder in verschiedenen Systemen verwendet, so stehen einem Angreifer nach Passwort-Diebstahl die Türen zu allen möglichen Services wie Finanzdienstleistungen, Mailkonten oder den sozialen Medien offen. Aber passiert das wirklich? Ja! Bereits heute befinden sich Milliarden von Passwörtern im Umlauf. Über 550 Millionen Passwörter sind allein in einem einzigen öffentlichen Verzeichnis hinterlegt. Die Zahl der tatsächlich geklauten Passwörter dürfte um Längen grösser sein. Denn unerlaubt an ein Passwort zu gelangen, ist einfach und die finanzielle Attraktivität gross: durch das Mitschneiden des Datenverkehrs in einem Netzwerk, durch Schadsoftware, das Ablesen von Passwörtern von Zetteln und unsicheren Notizen (z.B. während TV-Aufnahmen), durch manuelles Raten von unsicheren Passwörtern, systematisches Ausprobieren (brute force), Mitlesen bei der Eingabe (sog. Schulter-Surfen), durch unsichere Speicherung und diverse Formen des Social Engineerings.

Passwort-Manager helfen nur bedingt

Das oft gepredigte Credo, ein jeder möge seine Passwörter nicht wiederverwenden, lässt sich in der Praxis bequem durch Passwort-Manager realisieren. Doch Vorsicht! Solch eine Software zur Verwaltung von Passwörtern legt alle Eier in einen Korb, und das kann böse enden: Sichert die Applikation die Passwörter ungenügend, sind plötzlich alle Passwörter einem hohen Risiko ausgesetzt. Darüber hinaus helfen Passwort-Manager nicht gegen die Verwendung von kurzen oder einfach zu erratenden Passwörtern. Und schliesslich müssen die Passwörter zwischen allen eigenen Geräten (Laptop, Tablet, Smartphone) ausgetauscht werden, um wirklich einen sinnvollen Mehrwert zu bieten. In diesem Fall gelangen die Passwörter meist unweigerlich in die Cloud – zwar idealerweise verschlüsselt, aber eben deutlich exponierter.

Was also tun, wenn man einem Passwort-Manager nicht vertrauen möchte? Was tun, wenn im Unternehmensnetzwerk keine synchronisierten Passwort-Manager zugelassen sind? Dieser Beitrag stellt eine Möglichkeit vor, sich unbegrenzt viele, und dennoch eindeutige und zugleich komplexe Passwörter im Kopf zu merken.

Doch zuerst einen Schritt zurück: Einfache und kurze Kombinationen erhöhen das Risiko

Obwohl heute den Meisten klar sein dürfte, dass leicht zu knackende Kennwörter nicht mehr verwendet werden sollten, zeigt die 2018 von SplashData durchgeführte Studie, dass die

Kombinationen «123456» und «password» weiterhin Platz eins und zwei der am häufigsten verwendeten Passwörter belegen. Auch simple Tastenkombinationen wie «qwerty» oder «admin» stehen bei den Usern ganz oben auf der Liste – für Hacker ein gefundenes Fressen. Der oftmals gesäte Ratschlag, Passwörter zu generieren, die sich aus den Anfangsbuchstaben eines Merksatzes wie «Meine Oma isst am Sonntag gerne Kuchen» ableiten, bietet zwar eine Möglichkeit, den Schwierigkeitsgrad der Passwortkombination zu erhöhen, löst aber nur einen Teil des Problems; nämlich das der Komplexität, nicht aber das Problem der Wiederverwendung und der Gefahr von Wörterbuchangriffen.

Zudem geht nichts über die Länge eines Passworts. Warum? Der Suchraum für Hacker muss möglichst gross gehalten werden. Angenommen, unsere Passwörter bestehen aus Gross- und Kleinbuchstaben (26 + 26 Zeichen), Sonderzeichen (33 Zeichen) und Ziffern (10 Zeichen). Dann gibt es 95 mögliche Symbole pro Stelle. Bei Passwortlänge 8 ergibt das 95^8 = 6.7 x 10^15 verschiedene Möglichkeiten. Der Suchraum, um alle Passwörter systematisch zu testen besteht also aus einer Zahl mit 16 Stellen. Auf modernen Systemen lässt sich ein Passwort mit 8 Stellen systematisch in etwas mehr als einer Minute knacken. Verwendet man stattdessen 9 Zeichen, dann braucht es schon 95-mal länger, also ungefähr zwei Stunden. Bei 10 Zeichen ist es eine Woche, bei 11 Zeichen schon fast 2 Jahre. Und bei 12 Zeichen steigt die Zahl auf knapp zwei Jahrhunderte. Passwörter mit 12 Zeichen sind also bestens vor Brute-Force-Angriffen geschützt – sofern der Suchraum nicht künstlich durch Vornamen, Städte oder andere Begriffe, die in Wörterbüchern stehen, eingeschränkt wird oder auf verschiedenen Plattformen wiederverwendet wird.

Die Essenz eines guten Passworts

Fassen wir zusammen: Um den Schutz vor dem Datenklau möglichst hoch zu halten, müssen im Umgang mit Passwörtern vor allem drei Grundsätze beachtet werden: Das Passwort sollte mindestens 12 Zeichen enthalten, schwer zu erraten sein, also keine persönlichen oder allgemeinen Rückschlüsse zulassen (siehe Liste der schlechtesten Passwörter), und für jede Plattform individuell sein. Wie also lassen sich viele unterschiedliche und zugleich sichere Passwörter generieren, ohne dass sie schriftlich festgehalten werden müssen? Hier ist eine Schritt-für-Schritt-Anleitung:

1) Starkes und unpersönliches Masterkennwort wählen

Im ersten Schritt sollte ein sicheres Masterkennwort generiert werden, das keinen direkten und offensichtlichen Bezug zum Nutzer hat (wie z.B. Name, Wohnort, Geburtsdatum, usw.). Hierfür eignet sich die eingangs erwähnte Methode der Zeichenkette, die sich aus einem Merksatz, einem Zitat, einer Stelle aus dem Lieblingsbuch, einem Songtext, o.Ä. ableitet. Das Masterkennwort wird dadurch beliebig, unpersönlich und einprägsam. Um die Länge von 12

Zeichen im Endpasswort sicherzustellen, sollte das Masterkennwort bereits aus einem langen Satz abgeleitet werden. Anstelle der Abkürzung eines Satzes könnte man auch den Satz selbst als Masterkennwort verwenden. In diesem Fall könnte der Satz kürzer sein, damit man auf mobilen Geräten noch immer in vernünftiger Zeit eine Eingabe durchführen kann. Aus den Anfangsbuchstaben des Merksatzes «Bei Stromausfall ist die Gelegenheit günstig, um mit dem Fön zu baden» ergibt sich beispielsweise das folgende Masterkennwort:

BSidGgmdFzb

Um die Stärke des Passworts zu erhöhen, sollte mindestens ein Sonderzeichen angefügt werden, z.B. ein Ausrufungszeichen:

BSidGg**!**mdFzb

2) Variationen des Masterkennworts kreieren

Der zweite Schritt besteht darin, das Masterkennwort für die einzelnen Services und Plattformen zu modifizieren. Das Konzept dazu ist denkbar einfach: Im Masterkennwort werden beliebige, aber fest gewählte Stellen mit unterschiedlichen Buchstaben und Zahlen ergänzt, die je nach Plattform variieren.

Schritt 1: Zum Beispiel könnte an der 3. Stelle immer **eine Zahl eingefügt werden**, die von der **Länge des Namen**s des aktuellen Service abgeleitet ist. Bei LinkedIn wäre das eine 8, da «LinkedIn» aus acht Zeichen besteht, bei Google und Zühlke eine 6. Die Modifikationen lassen sich je nach gewünschtem Schwierigkeitsgrad beliebig verändern. So können beispielsweise die Zahlen noch zusätzlich um einen beliebigen, aber festen Faktor multipliziert werden, oder eine beliebige, aber feste Zahl kann addiert werden. Nehmen wir also an, wir addieren die Zahl 3 dazu, ergeben sich folgende Zwischenpasswörter:

LinkedIn: BS**11**idGg!mdFzb
Google: BS**9**idGg!mdFzb
Zühlke: BS**9**idGg!mdFzb

Schritt 2: Das Zeichen an der X-ten Stelle des Zwischenpassworts wird durch ein **frei wählbares, aber festes Symbol ersetzt**. Die Stelle X ist dabei zum Beispiel die **Anzahl der Konsonanten** im Namen der Plattform, für die das Passwort generiert wird, multipliziert mit 2. Für LinkedIn wäre X also 10, da «LinkedIn» aus fünf Konsonanten besteht, für Google wäre es 6, für Zühlke wäre es 8. Das ersetzende Symbol könnte beispielsweise ein «@» sein. Man erhält also:

LinkedIn: BS11idGg!@dFzb
Google: BS9id@g!mdFzb
Zühlke: BS9idGg@mdFzb

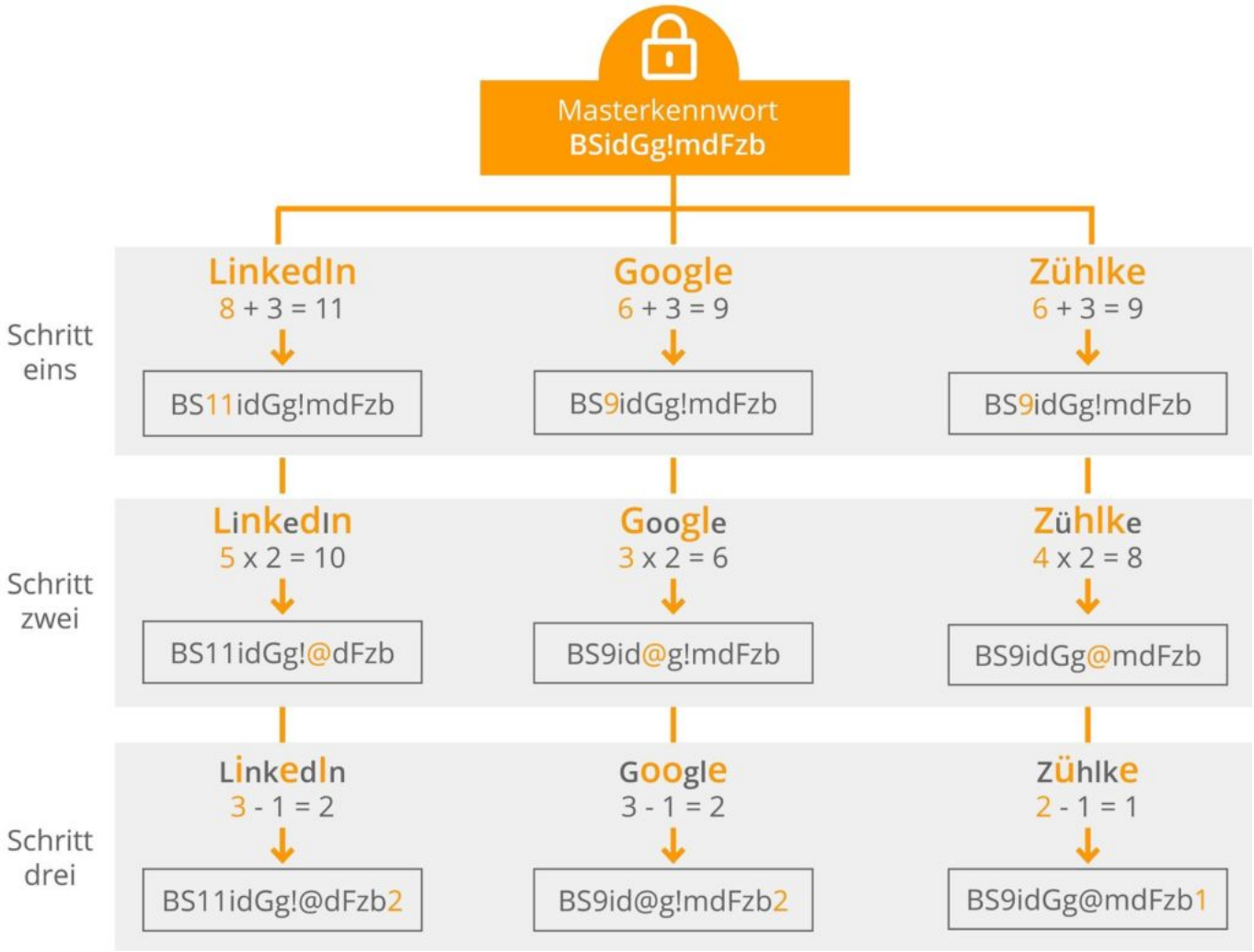
Auch hier ergeben sich zahlreiche Variationsmöglichkeiten, zum Beispiel könnte die Stelle um ein paar Zeichen nach links oder rechts verschoben werden. Auch sind andere Zeichen oder sogar Zeichenabfolgen denkbar.

Schritt 3: An der letzten Stelle des Passworts wird die **Anzahl der Vokale** im Namen des Services **angefügt**. Zur höheren Sicherheit könnte man die Zahl 1 subtrahieren. Für LinkedIn würde die Zahl 3-1=2 angehängt, da das Wort «LinkedIn» drei Vokale enthält.

LinkedIn: BS11idGg!@dFzb**2**
Google: BS9id@g!mdFzb**2**
Zühlke: BS9idGg@mdFzb**1**

Je nach persönlichem Sicherheitsbedürfnis können und sollten weitere Schritte dieser Art ergänzt werden. Wichtig ist, dass die Ableitungsschritte ausschliesslich vom Namen des Services abhängen, für das ein Passwort generiert werden soll. Je komplexer die Regeln und je mehr Variation sie hervorrufen, desto sicherer sind die resultierenden Passwörter. Die Addition, Multiplikation oder Subtraktion von Zahlenwerten kann weggelassen werden, wenn man nicht nach Konsonanten oder Vokalen fragt, sondern nach anderen kreativen Eigenschaften, beispielsweise nach der Zahl an «runden» Buchstaben (o, p, b, g, e) oder nach Buchstaben, die hinter einem bestimmten Buchstaben im Alphabet stehen (zum Beispiel hinter dem Buchstaben «r» stehen s, t, u, v, …).

Hier gibt es zahlreiche Möglichkeiten, welche die Individualität und somit die Sicherheit des Systems erhöhen. Die Ableitungsregeln dürfen – allerdings nie zusammen mit dem Masterkennwort – an einem sicheren Ort aufgeschrieben werden.



Fazit

Diese Methode bietet eine elegante und schlanke Möglichkeit, eine Fülle von einzigartigen Passwörtern zu schaffen, die weder einen Rückschluss auf das Masterkennwort noch auf die Plattform zulassen. Auch wenn die Passwörter auf den ersten Blick ähnlich aussehen, so sind sie nicht exakt gleich. Ähnliche Passwörter stellen – im Unterschied zu exakt gleichen Passwörtern – bei automatisierten Angriffen in der Regel kein Problem dar. Selbst wenn ein Angreifer zwei von dieser Methode abgeleitete Passwörter sieht, kann er kein gültiges Passwort für einen dritten Service ableiten.

Zudem lassen sich sowohl das Masterkennwort als auch die Variationen – sollten sie einmal vergessen gehen – immer wieder vom Ursprungssatz und dem Schlüssel ableiten, ohne dass die finalen Passwörter selbst irgendwo schriftlich festgehalten werden müssen. Auch wenn das Verfahren auf den ersten Blick komplex wirken mag, so erfolgt die Ableitung bei regelmässiger Anwendung innerhalb von wenigen Sekunden im Kopf und ist damit ähnlich schnell wie ein Passwort-Manager – nur sicherer.

So simpel die Massnahme von raffinierten Passwörtern im Kontext der firmeneigenen Informationssicherheit auch scheint – sie legt den Grundstein für eine wirkungsvolle Cyber-Defense, in der die Mitarbeitenden eine zentrale Rolle spielen. Denn sind die Menschen in einer Organisation genügend ausgebildet und sensibilisiert, sind sie nicht mehr Risikofaktor, und auch nicht das schwächste Glied in der Abwehrkette, sondern das bestmögliche Schutzschild gegen Cyber-Angriffe.