Version: 1v2

Eine theoretische Betrachtung zur Häufigkeit des Passwortwechsels

Die nachfolgende Erörterung soll die Aspekte abdecken, die sich ergeben, wenn man der Frage nachgeht, welchen Einfluß der Passwortwechsel auf die Sicherheit hat.

Es wird vorrausgesetzt, daß ein sicheres Passwort genutzt wird, zu welchem dem Angreifer keine weiteren Informationen vorliegen und welches nach technischem Stand als sicher betrachtet wird (also hinreichend lang ist und zufällig genung ist).

Ein Angreifer nutzt die sogenannte Brute-Force-Technik um das Passwort zu ermitteln.

1. Die Extremwertbetrachtung

1.1 Maximalwert
Das sichere Passwort kann im Rahmen einer Brute-Force-Attacke erst dann genackt werden, wenn sämtliche Möglichkeiten durchprobiert wurden (maximale Sicherheit des Passworts in Kombination mit dem Fall, daß beim ausprobieren sämtlicher möglichen Lösungen, die Letzte das Passwort ergibt).

1.2 Minimalwert
Dieser ist theoretischer Natur. Sofern man das Passwort so häufig wechselt, daß genau in dem Moment, in dem ein Passwort ausprobiert wird, genau das richtige Passwort auch im System als Passwort hinterlegt wurde, ist das System ebenfalls genackt.

Die "Haltbarkeit" des Passwortes liegt somit zwischen fast Null (Minimum) und der Zeit, die vergeht, bis man die maximale Anzahl an möglichen Passwörtern durchprobiert hat (Maximum).

2. Weitere Aspekte, welche Auswirkungen haben

2.1 Ungünstigster Aspekt des Passwortwechsels
Da man nicht weis, wie die Brute-Force-Attacke durchgeführt wird, ist es nicht ausgeschlossen, daß selbst kurz vor erreichen der letzten möglichen Kombinationen, ein Passwortwechsel nichts bringt, weil die Lösung im Rahmen der Brute-Force-Attacke nun durch den Angreifer trotzdem ermittelt wird. Das neue Passwort war ebend nicht seine letzte Variante, sondern die vorletzte, welche zum ausprobieren anstand. Das Passwort ist in kürze genackt.

2.2 Günstigster Aspekt des Passwortwechsels
Durch einen Passwortwechsel nutzt man ein Passwort, welches der Angreifer bereits probiert hat. Somit muß er weiterhin alle Möglichkeiten durchprobieren. Die Dauer hierfür liegt im Bereich der Maximalzeit oder sogar darüber hinaus.

Liegt die Wahrscheinlichkeit für das Eintreten der Situationen 2.1 oder 2.2 bei jeweils 50%?

Ich würde dies verneinen.

Je länger das Passwort um so größer der Anteil an qualitativ guten Passwörtern.

Auch hier wieder die Extrembetrachtung:

Ein Passwort mit einem Zeichen, welches evtl. nur aus den Ziffern 0 bis 9 bestehen darf, hat z.B. nur dann sieben "gute" Passwörter, wenn man vorraussetzt, daß die Ziffern 0, 1 und 9 als zu einfach angesehen werden. Somit sind 70% aller möglichen Passwörter gute Passwörter.

Ein langes Passwort hat auf Grund der Vielzahl an möglichen Passwörtern einen "Pool" an guten Passwörtern, der zwar auch nur 70% beträgt, jedoch auf Grund der Kombinationsmöglichkeiten hier nicht sieben Passwörter umfaßt (also 2...8) sondern ... mehr. Somit ist es für den Angreifer aufwendiger das richtige Passwort zu ermitteln, obwohl der Anteil weiterhin 70% beträgt. Anders veranschaulicht: Zum erraten des Passwortes ist die Chance richtig zu liegen bei einem aus sieben Passworten 1:6 (gerundet 17%). Bei 20 zulässigen Passwörtern und 70% Guten ist das Verhältnis 1:13 - die Wahrscheinlichkeit zufällig des Richtige zu erraten liegt bei rund 8%. Ob nun 70% oder nur 7% aller möglichen Passwörter gut sind, spielt hier keine Rolle, weil es in beiden Fällen gleich ist.

Ergebnis: Ein zeitlich gut platzierter Passwortwechsel erhöht die Sicherheit, weil (mit der Länge des Passwortes) die Wahrscheinlichkeit steigt, daß das neue Passwort evtl. in dem Bereich liegt, der bereits durch die Brute-Force-Attacke ausprobiert wurde. Somit ist das Eintreten von 2.2 wahrscheinlicher.

Folgender Aspekt spricht gegen einen häufigen Passwortwechsel:

Greifen wir das Beispiel mit den zulässigen Passwörtern 0...9 auf.
Hier haben wir sieben Passwörter (2...8) als "gute" Passwörter eingestuft.
Dies bedeutet, daß nach sieben Passwortwechseln nur noch "schlechte" Passwörter übrig bleiben. Alle guten Passwörter sind bereits verbraucht.

Bei einem langen Passwort ist die Anzahl der "guten" Passwörter höher.
Statistsich gesehen, verbraucht man bei jedem Passwortwechsel jedoch eines der "guten" Passwörter, sodaß immer weniger über bleiben. Durch den Passwortwechsel bröckelt also der Schutz.

Sollte es also keine weiteren Gründe geben, die für einen Passwortwechsel sprechen, so ist das zu häufige Wechseln des Passwortes eher nachteilig.

Hier kann man noch ein wenig „tricksen“, indem man z.B. ein gutes Passwort, welches man zuvor bereits nutzte, nochmals verwendet. Die widerholte Nutzung des selben Passworts ist jedoch in Fachkreisen „verpönt“. Dem mathematischen Aspekt ein Passwort nochmal zu nutzen wird hier nicht weiter nachgegangen.

Was bedeutet häufig oder selten nun konkret?

Bezugnehmend auf den Artikel

https://wiki.selfhtml.org/wiki/Sicherheit/sichere_Passwortwahl

werden Zeiträume von 72 Jahren und mehr angegeben, sofern das Passwort acht Zeichen umfaßt und die Brute-Force-Attacke eine Million Zeichen pro Sekunde ausprobieren kann. Ohne jetzt in den Bereich der höheren Mathematik einzutauchen, stellten wir fest, daß ein längeres Passwort in Kombination mit sinnvollen Wechselintervallen die Wahrscheinlichkeit für ein Erraten zu Gunsten des Passwortinhabers verschiebt.

Da der Aufwand zum erraten eines langen Passwortes exponentiell steigt, liegt die 50% Marke nicht bei 36 Jahren (also 50% der Zeit von 72 Jahren die zum erraten eines Passwortes mit acht Zeichen maximal benötigt werden würden), sondern eher im Bereich von 55-60 Jahren (bezogen auf die dem Artikel zu grundeliegende Rechenleistung).

In Anbetracht der ständig steigenden Rechenleistung, wird sich also das Zeitfenster für den Maximalwert von 72 Jahren verkürzen. Damit einhergehend wird auch die 50% Marke früher erreicht. Angenommen die guten Passwörter verteilen sich gleichmäßig um die 50% Marke, dann ist es sinnvoll zum Zeitpunkt der 50% Marke das Passwort zu wechseln. Auch dies nochmal veranschaulicht: Die im oben genannten Beispiel als gut titulierten Passwörter 2...8 verteilen sich genau 50:50 um den Mittelwert 5. Auch hier verzichte ich auf den Einsatz von höherer Mathematik, sehe jedoch keinen Grund, warum bei milliarden von Passwörtern hier die Verteilung von diesem 50:50 Verhältnis abweichen sollte.

Bezugnehmend auf das wahre Leben, könnte also ein frisch eingeschulter Grundschüler sein Passwort ohne Hektik im Renteneintrittsalter ändern, sofern man die 72 Jahre zu grunde legt; insbesondere wenn das Passwort qualitativ sehr gut ist und außerdem recht lang. Da die fortschreitende Rechenleistung, wie gerade geschildert, die Zeiträume verkürzt, könnte der 50%-Punkt derzeit (Stand des Jahres 2017) bei grob 40 Jahren liegen.

Wer per Anhalter durch die Galaxis unterwegs ist, könnte den Zeitraum von 42 Jahren für einen geeigneten Zeitpunkt ansehen ;-)
* Wer diese Anspielung auf einen Kultfilm versteht lächelt jetzt, alle anderen: bitte einfach ignorieren und weiterlesen! *

Häufigeres Ändern verschiebt die Wahrscheinlichkeit für einen unberechtigten Systemzugriff ja eher zu Gunsten des Angreifers. Den Aspekt des Risikos, das das Login inkl. Änderung des Passwortes auch ein Risiko birgt, betrachten wir nicht weiter.

Die Notwendigkeit ein gutes Passwort zu ändern ergibt sich somit eher dadurch, daß im realen Leben eine Situation eingetreten ist, bei der Ihnen jemand über die Schulter geschaut hat und somit Ihr Passwort kompromittiert wurde. Auch weitere, externe Einflüsse, wie Keylogger, welche auf dem von Ihnen genutzten System laufen oder sogenannte Man-in-the-middle-Angriffe stellen Faktoren dar, welche in der hiesigen Betrachtung zur Passwortwechselfrequenz nicht abschließend berücksichtigt werden können. Das Durchprobieren von millionen Passwörtern wird im Normalfall dadurch verhindert, daß die Systeme nach einer zuvor bestimmten Anzahl an Fehlversuchen den Login sperren oder weitere Schutzmaßnahmen greifen. Auch das NIST (National Institute of Standards and Technology) rät von regelmäßigen Passwortwechslen ab.

Vielen Dank!