Autor: Christian Kruse

Einleitung

Wer kennt das nicht: man hat sich bei einem neuen Service angemeldet, oder auf dem Server steht der monatliche Passwort-Wechsel an, und es fällt und fällt einem kein Passwort ein, das den Anforderungen des Sicherheits-Konzeptes genügt: entweder, es ist zu kurz, oder es ist nicht kryptisch genug, oder es ist zu kryptisch, und man kann es sich nicht merken. Schließlich, weil man keine Lust mehr hat, sucht man sich ein beliebiges, leider meist unsicheres Passwort aus.

Mit diesem kleinen Artikel möchte ich sowohl etwas mehr Sicherheitsbewusstsein wecken, als auch die Wahl eines sicheren Passworts durch das Verständnis, wie so ein Passwort aufgebaut ist, erleichtern. Ich will jedoch gleich vorneweg sagen: die Vergabe von sicheren Passwörtern erfordert viel Disziplin vom User selbst! Dieser Artikel kann und möchte keine Super-Methode zur Erstellung von sicheren Passwörtern vorstellen, denn wirklich sichere Passwörter gibt es nicht.

Warum Passwörter unsicher sein können

Warum ein Passwort unsicher (*weak*) sein kann, kann mehrere Gründe haben. Der einfachste z. B. wäre, dass es zu kurz ist: ein 2-Zeichen-Passwort hat (wenn man als valide Zeichen a-z, A-Z und 0-9 zugrunde legt) 62^2 (= 3844) mögliche Kombinationen. Sicher, für einen Menschen ist das sehr viel auszuprobieren, aber ein PC braucht dazu nur wenige Sekunden.

Ein weiterer Grund ist der Aufbau eines Passworts. So ist z.B. das Passwort "111" kein sehr sinniges Passwort. Einerseits ist es sehr leicht herauszufinden (auf die Tastatur schielen) und außerdem ist der daraus generierte Hash nicht sehr komplex.

Auch die Passwort-Analyse bietet einen Ansatz. Die Passwort-Analyse besteht im Grunde aus der Einschätzung der menschlichen Psyche und der Annahme, der Mensch sei ein Gewohnheitstier. Z.B. wird sehr gern die eigene Telefon-Nummer oder die Konto-Nummer als Passwort benutzt. Aber es gibt auch sehr beliebte Wörter, die Top drei aus der Liste dürften wohl "Gott", "Sex" und "Liebe" sein. Ebenfalls sehr beliebt sind Teile der E-Mail-Adresse und/oder Teile des Namens, der User-ID, etc. Dies sollten Sie alles vermeiden!

Warum ein sicheres Passwort wichtig ist

Viele Leute denken sich nichts bei der Vergabe von Passwörtern. Doch dabei ist dieser Vorgang enorm wichtig. Leider gibt es in unserer Gesellschaft Individuen, (Achtung, eigene Ansicht!) die nur auf ihr eigenes Wohl aus sind und sich dieses zum Nachteil anderer rücksichtslos beschaffen.

Das schönste Beispiel sind hier wohl die zahlreichen, aus dem Boden gestampften Webshops. Hier wird oft gedankenlos ein General-Passwort vergeben, das häufig auch noch sehr simpel aufgebaut ist. Dies ermöglicht es einem potentiellem Angreifer relativ einfach, Waren auf Ihren Namen zu bestellen — meist lassen sich solche Delikte zwar nachweisen, aber den Ärger haben Sie trotzdem damit.

Dieses Beispiel lässt sich auf viele andere Situationen übertragen, und es ist leider die Regel. Viel Computer-Kriminalität könnte vermieden werden, wenn mehr Endanwender ihren "inneren Schweinehund" überwinden und vernünftige Passwörter vergeben würden. Doch im gleichen Maß sind die Shop-Betreiber, Sicherheits-Beauftragten und andere, die für Passwortakzeptanz oder Passwortvorschläge zuständig sind, Schuld: ich habe bisher noch keinen Webshop mit Plausiblitätsprüfung des Passwortes gesehen.

Sicher werden jetzt viele sagen "Wer will schon ausgerechnet mir Böses?", oder "Wer will schon ausgerechnet **meine** E-Mails lesen?". Aber darum geht es ja gar nicht. Dem Angreifer ist es (meist) egal, wessen Account-Passwort er bekommt. Er interessiert sich auch nicht unbedingt für Ihre Mails. Ihn interessiert nur, wie er in das System hinein kommt. Denn hat er erstmal Zugriff, ist im Grunde der Krieg verloren.

Zweifellos ist es nervig, sich z.B. alle n Tage ein neues Passwort ausdenken zu müssen, nur weil ein Sysadmin oder Serverbeteiber das erzwingt. Aber gerade im Firmen-Umfeld hat sich erwiesen: ein Sicherheitskonzept ist immer nur so stark wie sein schwächstes Glied. Will heißen, wenn Sie ein sehr einfaches Passwort (oder vielleicht auch gar kein Passwort) verwenden, machen Sie es dem potentiellen Angreifer sehr leicht, in das Firmen-Netz einzudringen. Und **das** ist das eigentliche Problem: es geht in solch großen Netzwerken meist gar nicht darum, ob Ihre Privatsphäre hinreichend geschützt ist, sondern schlicht und ergreifend darum, dass das Firmen-Netzwerk geschützt ist.

Aufbau eines (relativ) sicheren Passworts

Ein sicheres Passwort besteht sinnvollerweise aus Groß- und Kleinbuchstaben sowie aus Ziffern. Es enthält keine (wahrnehmbare) Systematik und ist wenigstens (das ist überigens nur meine unerhebliche Meinung) 8 Zeichen lang. Es sollte kein Wort einer bekannten Sprache sein (z. B. Englisch, Deutsch oder Französisch). Außerdem sollte man für zwei Accounts **nie** dasselbe Passwort benutzen!

Sicherheits-Freaks neigen dazu, sogenannte "Tastatur-Hacks" zum Erzeugen von Passwörtern zu verwenden. Dabei handelt es sich um ein einmaliges, sinnloses und blindes Zehnfinger-Einhacken auf die Tastatur - und was dabei herauskommt, wird dann - ähnlich wie bei der Ziehung der Lottozahlen - als unumgängliches Gesetz und als **das** Passwort akzeptiert. Solche Passwörter sind natürlich extrem "sicher". Doch angesichts der Tatsache, dass sie beim Auswendiglernen und auch bei der Blind-oder Sterncheneingabe oftmals große Schwierigkeiten bereiten, sind sie nur scheinbar sicher. Denn wer z.B. in Anwesenheit anderer Personen ein Passwort eingeben muss, sollte das unauffällig und schnell tun können. Wer in einer solchen Situation auf das "Adlersystem" bei der Eingabe angewiesen ist, erleichtert den Anwesenden nur das unauffällige Mitverfolgen der eingegebenen Zeichenfolge. Oder noch schlimmer - er kann sich das supersichere Passwort gar nicht merken, notiert es sich irgendwo in Outlook oder dergleichen und muss es jedesmal über die Zwischenablage in die Eingabeaufforderung für das Passwort kopieren.

Gute Passwörter sollten also einen Mittelweg zwischen nicht erratbaren Zeichenfolgen und merkbaren Zeichenfolgen darstellen.

Wie lang sollte ein Passwort sein

Die Frage ist so leicht nicht zu beantworten. Das hängt vom Sicherheitsbereich ab. Generell kann man sagen, eine Mindestlänge von 8 Zeichen ist sinnvoll: 8 Zeichen bedeuten 191707312997281 Kombinationen bei der Zeichenklasse a-zA-Z1-9 (= 61 Zeichen). Das würde bei einer Million Tastenanschläge pro Sekunde eine Maximalzeit von ca. 53252 Stunden (191707312,997281 Sekunden) bedeuten (fast 6 Jahre). Das ist schon mal eine ganz ordentliche Zeit :-)

Bei höheren Sicherheitsbereichen (etwa Fimen-Netze oder dergleichen) würde ich auf 10 Zeichen Mindestlänge erhöhen (= 713342911662882601 Kombinationen, = ca. 198150808 Stunden oder ca. 22700 Jahre). Zur Einschätzung mal eine kleine Tabelle:

Mindestlänge	maximal benötigte Zeit (bei angenommener 1 Million Tastaturanschlägen pro Sekunde)
3 Zeichen	ca. 0,2 Sekunden
5 Zeichen	ca. 14 Minuten
8 Zeichen	ca. 53252 Stunden
10 Zeichen	ca. 1179469 Wochen
12 Zeichen	ca. 84168853 Jahre
15 Zeichen	ca. 19104730610573 Jahre

Doch nun kommt die Ernüchterung. Alle diese Angaben sind sogenannte **Maximalzeiten**! Maximalzeit bedeutet: wenn jemand in der angegebenen Geschwindigkeit versucht, das Passwort zu knacken, und erst die allerletzte eingegebene Zeichenkombination die richtige ist, dann dauert es so lange wie angegeben. Aber theoretisch könnte ja auch schon die allererste eingegebene Zeichenkombination richtig sein. Dann hat es nur eine hunderttausendstel Sekunde gedauert, um das Passwort zu knacken - trotz 15 Zeichen. Es kann also durchaus sein, dass ein Angreifer ein Passwort innerhalb weniger Sekunden herausgefunden hat. Zufall eben. Deshalb sollte man sich bei 8 Zeichen durchaus nicht in Sicherheit wägen. Außerdem kommt es auch auf die Rechenleistung an: hier wurde mit einer Millionen Tanstenanschlägen pro Sekunde gerechnet. Andere, bessere, später gebaute Rechner schaffen vielleicht das Millionenfache.

Die Anzahl der Kombinationen berechnet sich aus Zeichen-Anzahl$^{\text{Länge}}$: pro Zeichen kann das Passwort aus Zeichen-Anzahl Zeichen bestehen. Daraus ergibt sich bei einem Passwort von 3 Zeichen und einer Zeichenklasse von 62 Zeichen: 62 * 62 * 62 Kombinationen. Um die benötigte Zeit zu berechnen, dividieren Sie einfach durch die Anzahl der Tastenanschläge pro Sekunde — schon haben Sie die maximal benötigte Zeit in Sekunden.

Mit etwas Pessimismus könnte man nun sagen "ist doch scheißegal und alles wie beim Lotto". Doch zwischen der Maximalzeit und der theoretischen Chance, ein beliebiges Passwort mit nur wenigen Versuchen zu knacken, liegt der für potentielle Angreifer ziemlich ungemütliche "mittlere Bereich", der in der erdrückenden Mehrheit aller Fälle relevant ist - also der Bereich zwischen z.B. mehreren Tagen und mehreren Jahren. Und damit muss ein Angreifer zwangsläufig kalkulieren, wenn seine vielleicht anfänglichen Versuche, "nicht sichere" Passwörter zu probieren, fehlgeschlagen sind.

Natürlich sollte man auch noch hinzufügen, dass viele Zugangssysteme einen einloggenden Gast nach soundsoviel Fehlversuchen aus dem System werfen. Dann muss sich dieser, wenn er es wieder versuchen will, mit einer neuen

Identität, im Internet z.B. manchmal auch mit einer anderen IP-Adresse anmelden. Solche Dinge kann ein Angreifer allerdings bis zu einem gewissen Grad automatisieren.

Tipps zur Wahl eines (relativ) sicheren Passworts

Es wurde bereits gesagt, dass ein Passwort kein erkennbares System besitzen sollte. Diese Aussage kann man allerdings relativieren: es sollte kein durch eine Maschine erkennbares Muster besitzen. Wie Ihre Assoziationen zu einem Passwort sind, ist im Grunde völlig egal. Das gibt einem unverhoffte Freiheiten: wenn Sie jetzt z. B. ein Passwort zu einem Shell-Account oder Webshop brauchen, sehen Sie sich in der Umgebung um. Nehmen Sie den ersten Satz, der Ihnen zu einem Objekt in den Sinn kommt, nehmen Sie und packen den ersten Buchstaben jedes Wortes in das Passwort. Bei dem Satz "Ich telefoniere nicht besonders gern oder besonders häufig" wäre das z. B. dann die Zeichenfolge "itnbgnbh". Das sieht doch schon recht gut aus. Jetzt schreiben sie noch jeden n-ten Buchstaben groß: "iTNbgNBh". Nun schauen Sie noch, welche Buchstaben welchen Ziffern ähnlich sehen und ersetzen sie dadurch: "17NbgN3h". Und schon haben sie ein wunderschönes Passwort, das man sich mit Hilfe dieser sogenannten Eselsbrücke leicht merken kann.

Eine weitere Möglichkeit wäre auch, den Duden aufzuschlagen und zwei Wörter herauszusuchen (zwei x-beliebige) und die durch ein Satzzeichen getrennt miteinander zu verketten: "laufen:hunger". Auch hier sollte wieder eine Abstraktion durchgeführt werden (zuerst die Groß- und Kleinschreibung, dann die Ziffern): von "laufen:hunger" zu "LAufEN:hUNgeR" und schließlich zu "L4uf3N:hUNge4".

Letztenendes ist es auch relativ egal, wie Sie sich Ihr Passwort erstellen und merken. Wichtig ist nur, dass Sie die Regeln beachten, das Passwort nirgendwo aufschreiben und das, was am Ende herauskommt, kryptisch genug ist.

Alternativen

Die beste Alternative ist natürlich ein Passwort, das nur einmal gültig ist. Die meisten Online-Banking-Softwares arbeiten so: um eine Überweisung zu tätigen, muss man eine nur ein einziges mal gültige TAN eingeben. Andere Online-Banking-Systeme (z. B. das der CSFS, Credit Suisse Financal Services) benutzen zusätzlich Einweg-Passwörter. Dabei wird eine Key-Karte vergeben, in der ein Micro-Chip anhand der Zeit und einigen sehr komplexen Algorithmen ein Passwort erstellt, dass etwa 1 Minute lang gültig ist. Danach wird ein neues generiert. Der Hauptrechner im Rechenzentrum kann nachprüfen, ob der Code richtig ist — er verfügt auch über die Zeit und den Algorithmus. Diese ID muss zusätzlich zur User-ID und zum Passwort eingegeben werden.

Solche Passwörter zu knacken ist fast unmöglich. Sie sind meist 15-Stellig und besitzen Zeichen und Ziffern gleichermaßen — in Groß- und Kleinschreibung. Das Problem bei dieser Methode ist ein ganz anderes: die zeitliche Abstimmung mit dem Server :-) Wenn man z. B. eine langsame Internet-Anbindung hat oder in einem ungünstigen Augenblick versucht, sich einzuloggen, kann es durchaus passieren, dass das Passwort schon wieder ungültig ist.