Ronald Eikenberg

Sesam, öffne Dich nicht

Sicherheit von Passwörtern in Theorie und Praxis

Passwörter müssen nicht immer sehr lang, komplex und unmerkbar sein. Wichtiger ist es, viele verschiedene einzusetzen. Mit dem richtigen Konzept kann man sie sich trotzdem merken.

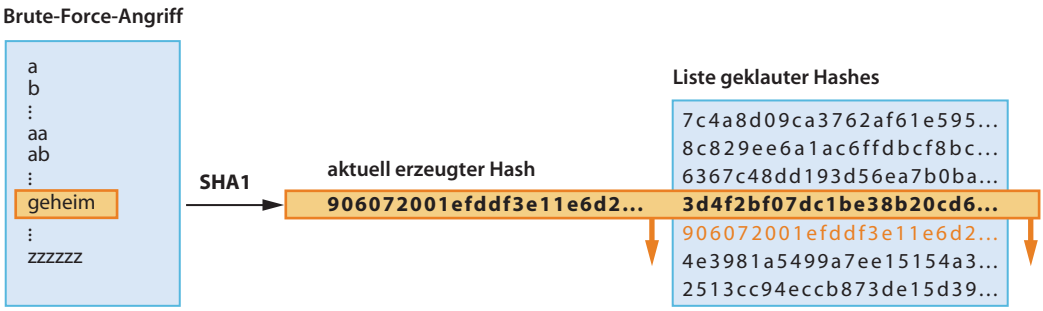
Jeder kennt die einschlägigen Tipps für gute Passwörter – trotzdem befolgt sie die breite Masse der Anwender nicht. Der Grund ist meist einfach: Die Anforderungen für ein sicheres Kennwort sind schlichtweg praxisuntauglich. Viele Aussagen zur Sicherheit von Kennwörtern sind zu pauschal, ohne den jeweiligen Einsatzzweck zu berücksichtigen. Ein langes Passwort ist schwer zu knacken? Nicht, wenn es aus Wörtern besteht, die man in jedem Duden findet. Passwortknacker spekulieren auf die Bequemlichkeit ihrer Opfer und probieren deshalb zunächst Wortlisten mit häufig genutzten Begriffen durch. Und wenn das Passwort aus einer kryptischen Zeichenfolge mit 24 Stellen besteht, dann ist es nicht nur unknackbar, sondern auch unmerkbar. Deshalb nehmen viele Anwender die Hilfe des Passwort-Managers im Browser in Anspruch – und handeln sich damit gleich wieder ein Sicherheitsproblem ein. Wer jedoch weiß, worauf es bei Passwörtern wirklich ankommt, kann sich sein persönliches Passwortkonzept basteln, das den jeweiligen Sicherheitsansprüchen genügt und das Gedächtnis trotzdem nicht überfordert.

Je nach Angriffsszenario genügt schon ein relativ einfaches, achtstelliges Passwort, um den virtuellen Brieftaschenklau wirkungsvoll zu vereiteln. Wenn ein Krimineller zum Beispiel ein Paypal-Passwort durch Ausprobieren über das Webfrontend knacken will, muss er Geduld mitbringen: Der Zahlungsanbieter sperrt potenzielle Angreifer bereits nach fünf Fehlversuchen für zwei Stunden aus. Um die über 722 Billionen möglichen Passwörter durchzuprobieren, die es mit zehn Sonderzeichen schon ohne Umlaute bei der vorgeschriebenen Mindestlänge von acht Zeichen gibt, würden über 30 Milliarden Jahre ins Land ziehen. Auch die vierstellige PIN der EC-Karte gilt trotz der lediglich 10 000 Möglichkeiten als sicher, weil man nur drei Fehlversuche hat, ehe die Karte gesperrt wird. Die größte Gefahr geht hier nicht von schwachen Passwörtern aus: Wo das Durchprobieren vieler Passwörter in kurzer Zeit nicht funktioniert, versuchen Kriminelle mit gefälschten Login-Seiten (Phishing) und Trojanern ihr Glück – und davor schützt leider auch das komplizierteste Passwort nicht.

Komplizierte Passwörter sind dann zwingend erforderlich, wenn Sie das Sicherheitsbewusstsein Ihres Gegenübers nicht einschätzen können. Durch Sicherheitslücken in Onlineshops, Foren und Content-Management-Systemen (CMS) gelangen immer wieder ganze Datenbanken in die falschen Hände. In diesem Fall müssen zuerst die Benutzer mit den schwächsten Passwörtern dran

user	mail	hash
admin	webmaster@	2513cc94eccb873de15d39773ce79e463682cb1c
rei	rei@ct.de	41a8a27e0e0c8b46832bb4f70d1d5f20d1a94ce5
otto	otto.normal@	7c4a8d09ca3762af61e59520943dc26494f8941b
sophia	junge.dame@	1e44882aa423942ede390caa32a3ae8a1b399fac
max	max@muste	6367c48dd193d56ea7b0baad25b19455e529f5ee

Blick hinter die Kulissen: Wie sicher ein Passwort beim Anbieter gespeichert wird, erfährt man in der Regel nicht.



Beim Brute-Force-Angriff erzeugt der Passwortknacker systematisch Hashes, die er mit der Liste der geklauten Hashes vergleicht.

glauben, denn von diesen gibt es nach wie vor jede Menge. Die Wahrscheinlichkeit, dass der Eindringling ausgerechnet das Passwort eines bestimmten Individuums knacken will, ist gering.

Rohe Gewalt

Hat der Angreifer erst mal die Datenbank einer Webseite in seinem Besitz, findet er dort im schlimmsten Fall direkt die Passwörter aller Anwender. Ob eine Website derartig schlampig mit den Kennwörtern umgeht, kann man etwa daran erkennen, ob man sich sein Passwort über die Funktion „Kennwort vergessen“ im Klartext zumailen lassen kann. Sicherheitsbewusstere Websites speichern nicht die Passwörter selbst, sondern lediglich nicht reversible Hashes. Hat ein Angreifer solche Hashes erbeutet, kann er sie zunächst einmal Google vorwerfen. Dort liefert etwa die Eingabe 906072001efddf3e11e6d2b5782f4777fe038739 sofort „geheim“ als Passwort.

Mehr Aufwand erfordert der systematische Ansatz, Hashes zu allen möglichen Zeichenkombinationen zu erzeugen und sie mit dem geklauten Hash zu vergleichen. Eine aktuelle Mehrkern-CPU schafft das über 38 Millionen Mal je Sekunde. Durch die Nutzung potenter Grafikprozessoren über Nvidias CUDA-Schnittstelle ist locker die sechsfache Geschwindigkeit drin [1]. Ein sechsstelliges Passwort, das die Groß- und Kleinbuchstaben, Ziffern sowie die zehn häufigsten Sonderzeichen – also 72 unterschiedliche Zeichen – enthalten könnte, ist mit GPU-Unterstützung in maximal neun Minuten geknackt.

Hätte das Passwort nur zwei zusätzliche Stellen, würde sich der Knacker bis zu 300 Tage die Zähne daran ausbeißen; nach 150 Tagen hat er die Hälfte aller Kombinationen durchprobiert und mit guter Wahrscheinlichkeit die richtige Lösung gefunden. Zwar kann der Angreifer in diesem Zeitraum mit geringem Mehraufwand gleich ganze Kolonnen der geklauten Hashes mit dem erzeugten Hash vergleichen, doch der aufzubringende Zeitaufwand ist trotzdem groß. Hat der Angreifer Zugriff auf einen ganzen Rechnerpark, ist es für ihn ein Leichtes, die Aufgabe zu verteilen, wodurch die Rechenleistung linear steigt. So werden beim Einsatz von 50 Rechnern aus den 150 Tagen nur noch drei und das Passwort ist plötzlich zum Greifen nah.

Wolkenbruch

Das ist nicht so weit hergeholt, wie es klingt. Durch Dienste wie Amazons Elastic Computing Cloud (EC2) hat jedermann die Möglichkeit, flexibel einen Rechencluster anzumieten und auf zu knackende Passwörter anzusetzen. Bezahlt wird nach Nutzungsdauer: Ein leistungsfähiger Cloud-Rechner mit Nvidia-GPU kostet gerade mal 2,10 US-Dollar je Stunde. Eine Grundgebühr gibt es nicht. Per Knopfdruck kann man weitere Systeme dazumieten, wodurch die Kosten unterm Strich nicht steigen – schließlich ist das Passwort auch entsprechend schneller geknackt.

Es kostet etwa 0,16 US-Dollar, ein gängiges sechsstelliges Passwort in der Cloud zu knacken. Ein achtstelliges Passwort würde schon mit rund 850 US-Dollar zu Buche schlagen. Spätestens ab einer Länge von zwölf Zeichen dürfte es für den Angreifer nicht mehr lohnen: Auf der Amazon-Rechnung stünden fast 23 Milliarden US-Dollar. Auch außerhalb der Wolke ist dieser Rechenaufwand kaum zu bewältigen: Eine durchschnittliche Grafikkarte wäre über eine Billion Jahre mit der Suche nach dem Passwort beschäftigt. Ein GPU-Rechencluster mit 1000 Maschinen wäre immerhin noch über eine Milliarde Jahre beschäftigt.

Man kann diesen Rechenaufwand erheblich reduzieren, indem man Tabellen mit vorberechneten Zwischenergebnissen der Hash-Operationen einsetzt. Die sogenannten Rainbow Tables [2] sind oft mehrere hundert Gigabyte groß und beschleunigen das Knacken eines Passworts etwa um einen Faktor 1000.

Das Salz in der Passwortsuppe

Allerdings greifen die Regenbogentabellen nur, wenn bei der Speicherung des Passworts kein Salt zum Einsatz kam, es sich also um den reinen Hashwert handelt. Beim Salting wird jedes Passwort mit einer zufälligen Zeichenkette, dem Salt, kombiniert. Daraus generiert die Anwendung dann den Hash, den sie zusammen mit dem Salt in der Datenbank ablegt. Das macht den Einsatz von Rainbow Tables in aller Regel praktisch unmöglich, da man für jedes Salt eine eigene der ohnehin riesigen Tabellen benötigte.

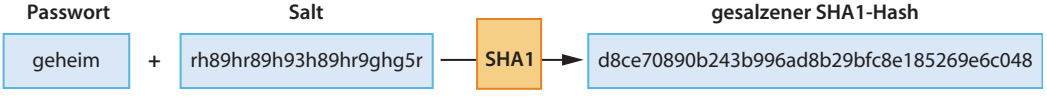
Als Anwender weiß man in den seltensten Fällen, ob die Passwörter gesalzen oder ungesalzen in der Datenbank einer Webseite landen. Im Zweifelsfall sollte man also mit dem Schlimmsten rechnen: damit, dass im Fall eines Einbruchs in die Website das Passwort kompromittiert ist, weil es entweder ungesalzen oder gleich im Klartext abgespeichert war. Viel wichtiger, als maximal komplizierte Passwörter zu verwenden, ist es somit, nicht auf allen Seiten das gleiche Passwort einzusetzen. Sonst kann der Einbrecher nicht nur den Account auf der ohnehin gehackten Website missbrauchen sondern sich mit diesem Passwort auch auf andere Dienste weiterhangeln.

Passworttresor ohne Tür

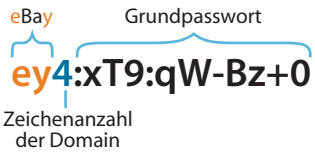
Wer deshalb für jede Seite ein eigenes Passwort verwendet und die dann mit dem Passwortmanager des Browsers verwaltet, hat an anderer Stelle ein Problem: Die Browser sichern die gesammelten Zugangsdaten in der Standardkonfiguration nicht ausreichend. Bei den aktuellen Versionen von Internet Explorer und Opera konnten wir mit Hilfe kostenloser Tools sämtliche gespeicherten Passwörter im Klartext anzeigen lassen – bei Firefox und Chrome klappt das sogar ohne Hilfsmittel.

Ein gefundenes Fressen für neugierige Kollegen, die sich in der Mittagspause an fremden PCs zu schaffen machen wollen. Zumindest im Fall von Firefox schützt auch ein gesperrter Windows-Rechner nicht vor unerwünschten Einblicken, denn wenn jemand das Kennwort des Benutzerkontos entfernt oder überschreibt, etwa mit der Boot-CD ntpasswd, ist auch der Weg zu den im Browser hinterlegten Passwörtern frei. Bei allen Browsern hat Schadsoftware, die sich im Rechner eingenistet hat, quasi direkten Zugang zum gesamten Passwort-Potpourri. Da ist es schon fast besser, die Passwörter mit den dazugehörigen Benutzernamen und URLs mit Klebezettelchen an den Monitor zu heften. Da kommt dann wenigstens der Trojaner nicht dran.

Zudem können Angreifer die automatisch ausgefüllten Login-Felder bei Firefox und Chrome leicht aus der Ferne auslesen, wenn die Website eine sogenannte Cross-Site-Scripting-Lücke aufweist – was leider viel zu oft vorkommt. Opera macht es dem Angreifer in diesem Fall



Gesalzen: Ein Salt wird mit dem vom Nutzer gewählten Passwort kombiniert, ehe daraus der Hash generiert wird. Das macht den Einsatz von Rainbow Tables praktisch unmöglich.



Mit einem einfachen System erzeugen Sie sichere seitenabhängige Passwörter, die Sie schnell rekonstruieren können.

Seite	Dienstteil	Grundpasswort	Passwort
eBay.de Google.de heise.de	→ ey4 ge6 he5	+ :xT9:qW-Bz+0 :xT9:qW-Bz+0 :xT9:qW (verkürzt)	= ey4:xT9:qW-Bz+0 ge6:xT9:qW-Bz+0 he5:xT9:qW

Wer Zugriff auf den PC hat, kann die im Browser gespeicherten Passwörter auch im Klartext auslesen.

etwas schwerer, da es die gespeicherten Formulardaten erst nach einem Klick auf das Schlüsselsymbol ausfüllt und anschließend automatisch abschickt. Der IE wartet mit der Passworteingabe zumindest, bis sich der Anwender für einen Login entschieden hat.

Gewusst wie

Allerdings kann man Firefox und Opera zu einem verantwortungsvollen Umgang mit Passwörtern bewegen: Legt man in den Optionen ein Masterpasswort fest, verschlüsselt der Browser die während der Surf-Ausflüge gesammelten Passwörter fortan. Anschließend fragt der Browser beim ersten Zugriff auf den Passwortspeicher nach dem Masterpasswort – Opera fragt auf Wunsch auch nach einem wählbaren Zeitraum erneut nach. Mit gesetztem Masterpasswort liefen unsere Recovery-Tools bei der Suche nach dem Klartextpasswort ins Leere.

Zumindest die Browser-basierten Angriffe funktionieren nicht mehr, wenn man einen getrennten Passworttresor wie KeePass oder SplashID verwendet. Aber auch da bleibt das Problem, dass man alle wichtigen Passwörter an einer Stelle speichert, die prinzipbedingt nicht ausreichend gegen Trojaner gesichert ist. Wenn der Anwender den Tresor öffnet, kann ein Spionageprogramm das Masterpasswort mitlesen und anschließend alle gespeicherten Passwörter auf einmal abgreifen.

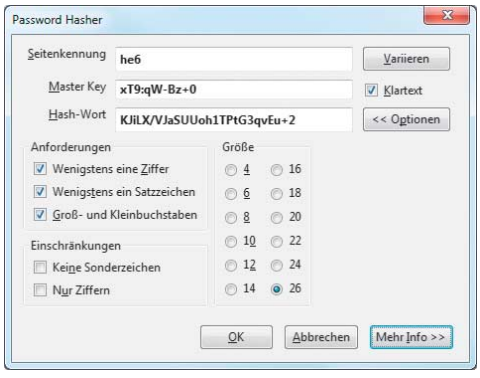
Da ist schon der einfache „Zetteltresor" deutlich sicherer. Der Trojaner, der Zugriff auf die sorgsam im Geldbeutel verwahrte Passwortliste erlangt, muss erst noch geschrieben werden. Es bleibt natürlich die Gefahr, dass man das Portemonnaie verliert oder es gestohlen wird.

Kennste eines, kennste alle

Deshalb ist es besser, die Passwörter erst gar nicht aufzuschreiben oder abzuspeichern, sondern sich einzuprägen. Dabei hilft ein einfaches System, mit dem man für jede Webseite ein eigenes Passwort erzeugt, das Sie sich gut merken und notfalls jederzeit rekonstruieren können.

Das System beruht darauf, sich einmalig ein kompliziertes Grundpasswort auszudenken und es mit einem seitenabhängigen Dienstteil zu verknüpfen. Den Dienstteil können Sie zum Beispiel aus dem ersten und den letzten Buchstaben des Domainnamens ohne Endung sowie dessen Länge erzeugen. Aus dem einmalig gelernten Grundpasswort „:xT9:qW-Bz+0" wird beim Google-Account etwa „ge6:xT9:qW-Bz+0" und bei eBay „ey4:xT9:qW-Bz+0".

Das Grundpasswort haben Sie nach mehrmaligem Wiederholen schnell intus. Variieren Sie diese Anleitung zu einem individuellen Konzept. Wichtig ist, dass nicht ohne Weiteres erkennbar ist, welcher Teil des Passworts der seitenbezogene Dienstteil ist. So haben Plünderer, die mit erbeuteten Passwörtern von Seite zu Seite ziehen, kaum noch eine Chance. Damit Ihr Grundpasswort nicht in falsche Hände gerät und Sie im Alltag weniger tippen müssen, können Sie es für weniger wichtige Seiten auch abkürzen. Für das Taucherforum, dessen Datenbank möglicherweise nur unzureichend geschützt ist, verwenden Sie beispielsweise das verkürzte Grundpasswort „:xt9:qW".



Die Firefox-Erweiterung Password Hasher erzeugt sichere Passwörter, die man sich ohne die Erweiterung jedoch nur schwer merken kann.

Passwörter mit System

Auf eine Abwandlung dieses Verfahrens setzt die Firefox-Erweiterung Password Hasher, die unter dem Link am Ende des Artikels zum Download bereitsteht. Sie klinkt sich in die Passworteingabefelder sämtlicher Webseiten ein und generiert anhand eines Grundpassworts und einer Seitenkennung eine Site-spezifische Zeichenkette, die bis zu 26 Zeichen lang sein kann. Die Seitenkennung kann man frei wählen. Standardmäßig verwendet die Erweiterung den Domainnamen der Seite ohne Endung, man kann sie aber auch nach einem Schema wie oben vorgestellt selbst erstellen. Das generierte Passwort ist ein Hash aus der Kombination von Seitenkennung und Grundpasswort. Gegenüber der manuellen Methode hat dies den Vorteil, dass weder der gleichbleibende noch der seitenspezifische Teil des Passworts im Klartext übertragen oder gespeichert wird.

Selbst wenn das erzeugte Passwort einem Angreifer in die Hände fällt, kann er nicht unmittelbar auf das verwendete System – und somit auf die auf anderen Seiten eingesetzten Passwörter – schließen. Der Nachteil dieser Erweiterung ist, dass man damit auf Systeme beschränkt ist, auf denen man Firefox mit der passenden Erweiterung verwenden kann. Da die erzeugten Hashes jedes Mal komplett anders sind, ist es nahezu unmöglich, sich mehrere davon zu merken, um sie etwa an einem anderen Rechner oder einem Mobilgerät einzugeben. Außerdem muss man der Versuchung widerstehen, den Passwort-Tresor von Firefox zu verwenden, der sonst wieder einen zentralen Angriffspunkt darstellt.

Fazit

Die Sicherheit eines Passworts ist nicht allein von dessen Komplexität abhängig. Den größten Sicherheitsgewinn erzielt man, indem man das Passwort seitenabhängig variiert. Und das ist mit dem oben vorgestellten System ganz einfach. Ist der PC mit einer Spionagesoftware infiziert, hilft jedoch selbst das ausgefeilteste Passwort nicht mehr. Die Gefahr durch Phishing können Sie durch das Variieren der Passwörter jedoch zumindest eindämmen: Haben Sie Ihre Login-Daten versehentlich in eine gefälschte Seite eingegeben, kann der Passwortdieb mit seiner Beute immerhin nicht von Seite zu Seite ziehen – und Sie müssen anschließend nur ein Passwort ändern. Auch in öffentlichen WLAN-Netzen könnten potenzielle Datendiebe lauern. Wie Sie sich vor Passwort- und Cookie-Klau im WLAN schützen, zeigen die FAQ „WLAN sicher nutzen" in c't 24/10. (rei)

Literatur

[1] Stefan Arbeiter, Matthias Deeg, Bunte Rechenknechte, Grafikkarten beschleunigen Passwort-Cracker, c't 06/09, S. 204

[2] Karsten Nohl, Kunterbuntes Schlüsselraten, Von Wörterbüchern und Regenbögen, c't 15/08, S. 190

[3] Ronald Eikenberg, FAQ: WLAN sicher nutzen, c't 24/10, S. 172

www.ct.de/1102150 c't