Geheime Schlüssel

Das Dilemma mit den Passwörtern kennen alle: Sollen sie sicher sein – oder möglichst gut zu merken? Mit unseren Tipps ist beides möglich.

ILLUSTRATION RICHARD DOWNS

● ***von Beat Rüdt***

Ein ganz normaler Tagesbeginn: Aufstehen, Handy einschalten, – PIN-Code eintippen –, E-Mails checken – Passwort eingeben –, auf dem Weg zur Arbeit Geld abheben beim Bancomaten – Code eintippen –, beim Znüni einkaufen den Punktestand der Coop-Profitcard abfragen – Code eintippen –, das elektronische Schloss des Firmeneingangs öffnen – Code eintippen – und schliesslich das Einloggen in den Bürocomputer mit – na was wohl? – einem Passwort. Innert einer Stunde gibt ein ganz gewöhnlicher Arbeitnehmer nicht weniger als sechs verschiedene Codes und Passwörter ein.

Damit nicht genug: Wer das Internet nicht nur zum Surfen in Anspruch nimmt, dem werden noch mehr PIN-Codes (PIN: Persönliche Identifikationsnummer) und Passwörter aufgehalst. Zahllose Dienste verlangen eine Identifikation: Einwahl ins Internet, E-Mail, Shopping-Seiten, Online-Banking, Auktionsseiten, Webserver und so weiter.

All diese Passwörter und PIN-Codes, oft in Verbindung mit einem Benutzernamen oder einer Karte (Bankkarte), dienen der eindeutigen Identifikation für sensible Bereiche. Die Buchstaben- und Zahlenkombinationen sollten deshalb möglichst so gewählt sein, dass eine Drittperson sie nicht durch Erraten herausfinden kann. Die Kehrseite: Je komplizierter ein Passwort ist, desto leichter vergisst man es.

Ein gutes Passwort hat mindestens acht Zeichen, besteht aus gross- und kleingeschriebenen Buchstaben, Zahlen und Sonderzeichen (z. B. «3Rt-4IiL» (siehe Box «Was ist Ihr Passwort wert?», S. 44). Für jeden Dienst sollten Sie aus

```
kidj8smKHGkkl;lßsk;.308fk:;&/ko9/g34hj 1
sKIUo0(6639)io,msiOPUIGmjislkla),mkrisk
),mkiw,s()=:;IOki)8u67sjuiskoUKlko097&(
/)oskiksl)8fks8kJuielsu572lpksljski386j
sl49kclw949mvlsejmksUi9K;KIuek1068Mk.so
Llw=opw12Sjri()lsikidj8smKhGkkl;lßsk;.3
08fk:;&/ko9/g34hjlsKiUo0(6639)io,msiOPU
IGmjislkla),mkrisk),mkiw,s()=:;IOki)8%6
7sjuiskoUKlko097&(/)oskiksl)8fks8kJuiEl
su572lpksljskki386jsl49kclw)49mvlsej(ksU
i9K;KIuek1068Mk.soLlw=opw12Sjri()lskidj
8smKhGkkl;lßsk;.308fk:;&/ko9/p34hjlsKIU
o0(6639)io,msiOPuIGmjislkla),mkroisk),m
kiw,s()=:;IOki)8q67sjuiskoUKlko097&(/)o
skiksl)8fks8kJuielsu572lpksljski386jsl4
9kclw949mvlsejmksUi9K;KIuek1068Mk.soLlw
=opw12Sjri()lsiekidj8smKjGkkl;lßsk;.308
fk:;&/ko9/)34hjlsKIUo0(6639)io,msiOPUIG
mjislkla),mkrisk),mkiw,s()=:;IOki)8(67s
juiskoUKlko097&(/)oskiksl)8fks8kJuiepsU
572lpksljSki386jsl49kclw949mvlsejmksUi9
```

Die roten Markierungen kennzeichnen mögliche Passwörter. Auf einer solchen Karte dürfen die Markierungen natürlich nicht aufgebracht werden.

Passwörter

Sicherheitsgründen ein separates Passwort wählen, das Sie zudem alle paar Monate wechseln müssen.

So weit die Theorie. Sich all das zu merken, ist aber ein Ding der Unmöglichkeit. Deshalb verwenden viele Nutzer Daten oder Namen als Passwörter, die sehr schnell mit einer Brute-Force-Attacke geknackt werden, siehe Abschnitt «Windows-Passwort vergessen», S. 44.

Passwörter merken

Keine Angst: Trotz unserer Unfähigkeit, uns verschiedenste komplizierte Passwörter zu merken, gibt es einige Strategien, die zum erstrebten Erfolg führen. Allerdings haben alle ihre Vor- und Nachteile.

Strategie: Wenige Passwörter

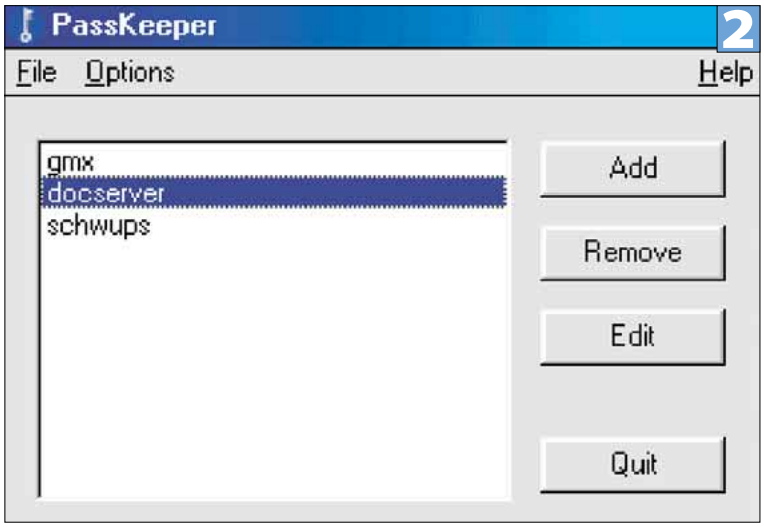
Sie generieren nur wenige Passwörter, zum Beispiel eines für alle Online-Dienste und eines für alle Bankkarten.
Vorteil: Sie merken sich nur noch zwei Passwörter; auch komplizierte Zeichenkombinationen lernen Sie spielend auswendig.
Nachteil: Ist das Passwort geknackt, hat der Angreifer Zugriff auf all Ihre Daten.
Bewertung: Diese Methode ist schlecht. Nutzen Sie sie nur, wenn Sie mindestens monatlich Ihre beiden Passwörter ändern.

Strategie: Passwörter aufschreiben

Sie schreiben alle Passwörter auf ein Blatt Papier.
Vorteil: Sie tragen die wichtigsten Passwörter immer mit sich herum. Ein Blick auf das Blatt genügt, und Sie wissen, welche Kombination zu welchem Dienst gehört.
Nachteil: Wird die Liste geklaut, hat der Dieb Zugang zu all Ihren gesicherten Diensten. Noch schlimmer ist es, wenn Sie die Liste direkt neben dem Computer ablegen. Das ist, als ob Sie die Wohnung verlassen und die Haustüre weit offen lassen würden.
Bewertung: Die schlechteste aller Möglichkeiten. Ist die Liste einmal weg, hat nur noch der Dieb Zugriff. Wenn Sie schon auf die Papierliste vertrauen (vielleicht, weil Sie die Passwörter immer mit sich herumtragen müssen), tarnen Sie diese mit vielen Füllwörtern, damit sie nicht auf den ersten Blick erkennbar ist (z. B. als Einkaufsliste).

Strategie: Der Merk-Zettel

Sie schreiben auf ein Blatt in horizontalen und vertikalen Linien Hunderte von Buchstaben, Zahlen und Zeichen, **Screen 1**. Für jeden geschützten Dienst generieren Sie ein Passwort, das, von einem Buchstaben ausgehend, in vertikaler, horizontaler oder schräger Richtung zusammengesetzt wird. Die roten Linien dürfen Sie keinesfalls auf dem Blatt einzeichnen. Falls Ihnen die Karte abhanden kommt, ist es für den potenziellen Datendieb sehr schwierig, die richtige Kombination herauszufinden.



PassKeeper bewahrt Ihre Passwörter auf.

Vorteil: Sie können ohne grosses Risiko Ihre komplizierten Passwörter mit sich herumtragen. Die Karte ist nicht sofort als Passwortliste erkennbar.
Nachteil: Ist bei vielen Passwörtern kompliziert, da Sie sich genau merken müssen, welches Kennwort zu welchem Dienst gehört und wo die Startpunkte liegen. Diese Methode ist nur anwendbar, wenn Sie das Passwort selbst auswählen dürfen.
Bewertung: Eine gute Möglichkeit für Leute mit sehr vielen verschiedenen Passwörtern.

Strategie: Verschlüsselte Datei

Sie speichern alle Passwörter in einer verschlüsselten Datei auf dem Computer. Sie benötigen nur ein Passwort, um an alle anderen Passwörter zu gelangen.
Beispiel: Auf der PCtip-Website finden Sie das Gratis-Programm PassKeeper (**http://www.pctip.ch/downloads/dl/16733.asp**). Es speichert und verschlüsselt Ihre Passwörter. Vor dem Abrufen der Einträge müssen Sie ein Passwort eingeben. Das Programm ist so klein, dass es auf einer Diskette Platz hat. Wenn Sie wollen, tragen Sie so Ihre Passwörter immer auf sich, **Screen 2**.
Vorteil: Sie müssen sich nur ein Passwort merken.
Nachteil: Ein potenzieller Angreifer muss nur ein Passwort knacken, um an alle Ihre Passwörter zu gelangen.
Bewertung: Sicher, sofern das Programm mit einem guten Passwort geschützt ist und Sie sich nicht auf eine einzige Diskette verlassen.

Strategie: Passwort im Buch

Sie nehmen ein beliebiges Buch, schlagen irgendeine Seite auf und stellen ein Passwort zusammen, das sich zum Beispiel aus den ersten Buchstaben jeder Zeile zusammensetzt.
Vorteil: Sie können jederzeit nachschauen, wie das Passwort lautet.
Nachteil: Sie müssen das Buch immer in Ihrer Nähe haben und dürfen die Seite nicht vergessen.
Bewertung: Eine aufwändige, aber gute Lösung. Sie generieren zufällige Passwörter und können diese immer nachschlagen.

Warnung

Die dümmsten Passwort-Sünden

Das Hacken von guten Passwörtern nimmt sehr viel Rechenkapazität und damit auch Zeit in Anspruch. Meist machen sich Angreifer aber gar nicht die Mühe, das Passwort effektiv zu knacken. Warum viel Zeit verschwenden, wenn man mit einem einzigen Anruf die gewünschten Daten bekommt?

Diese Methode nennt sich «Social Engineering». Der Hacker ruft die Hauptnummer einer Firma an und verlangt den Systemadministrator. Dann gibt er sich als Techniker des Unternehmens aus, das zum Beispiel die Firewall geliefert hat, und behauptet, er müsse für Wartungsarbeiten auf die Firewall zugreifen. Damit er das tun kann, verlangt er vom Systemverantwortlichen Benutzername und Kennwort, und schon kann er ins Unternehmensnetzwerk eindringen. Ähnliche Fälle sind auch im privaten Bereich bekannt: Ein Anrufer gibt sich als Bankangestellter aus, der auf Ihr Online-Banking-Konto zugreifen will. Er verlangt Benutzername, Passwort und Streichlistencode und leert Ihr Konto.

Doch gut geschulte Administratoren fallen nicht mehr auf diesen Trick herein. Aber auch das ist für den Hacker kein Problem. Er besucht den Firmensitz persönlich, gibt sich als Heizungstechniker aus, wandert ins Büro der Systemadministratoren und findet dort in den meisten Fällen eine Passwortliste mit allen relevanten Passwörtern direkt auf dem Pult. Sicherheitsexperten vermuten, dass dieser Trick in bis zu 70 Prozent aller Fälle funktioniert!

Ein weiterer schlimmer Fehler ist, wenn sich Anwender gar nicht die Mühe machen, das von der Herstellerfirma vorkonfigurierte Passwort zu ändern. Viele Attacken gelingen ganz einfach durch die Eingabe von Passwörtern wie «test», «Administrator», «admin» oder «1234».

Strategie: Hilfe vom Hilfssatz

▶ Sie wählen Passwörter, die Sie sich mit einem Hilfssatz merken können (z. B. IgpW2MzB für «Ich gehe pro Woche 2 Mal zur Bank»).
Vorteil: Sicheres Passwort, das Sie sich trotzdem leicht merken können.
Nachteil: Sie müssen sich für jeden Dienst einen Satz ausdenken, den Sie auch wirklich zuordnen können.
Bewertung: Dies ist eine der sichersten Methoden, wenn nirgendwo etwas schriftlich vermerkt ist.

Verlorene Passwörter finden

Trotz des oben genannten Tricks kann es passieren, dass Sie einmal ein Passwort vergessen. Je nach Situation ist es mehr oder weniger einfach, wieder an die verlorenen Daten zu kommen.

Szenario: Online-Passwort vergessen

Ein Webdienst – z. B. für Ihre E-Mails – ist nur mit Benutzername und Passwort abrufbar. Sie wissen zwar noch den Benutzernamen, das Passwort ist Ihnen aber abhanden gekommen.
Lösung: Viele professionelle Dienste bieten gleich unter dem Login-Fenster einen Link PASSWORT VERGESSEN? oder Ähnliches an. Hinter diesem Link wird ausführlich erklärt, wie Sie an Ihr altes oder ein neues Passwort kommen. Falls Sie beim Registrieren des Dienstes eine E-Mail-Adresse angegeben haben, wird das Passwort an diese Adresse gesandt. Bei einigen Diensten hinterlegen Sie eine so genannte «Sicherheitsfrage» mit zugehöriger Antwort. Geben Sie auf die Frage die korrekte Antwort, wird das Passwort entweder angezeigt oder zugestellt, **Screen 3**.

Szenario: Windows-Passwort vergessen

Sie haben auf einem Windows-Rechner mehrere Benutzer eingerichtet, wissen aber nicht mehr, welches Passwort zu welchem Benutzernamen gehört.

Online-Dienstleister erklären meist genau, wie der Nutzer an sein verlorenes Passwort kommt.

Hintergrund

Was ist Ihr Passwort wert?

Die Qualität eines Passwortes hängt von zwei Faktoren ab: Der maximalen Länge des Passwortes und der Anzahl der möglichen Zeichen. Diese zwei Werte bestimmen die höchstmögliche Zahl verschiedener Passwörter. Entsprechend viele Versuche müssten maximal unternommen werden, um ein Passwort zu knacken. Die Anzahl möglicher Kombinationen ergibt sich aus Anzahl Zeichen hoch Länge des Passwortes.

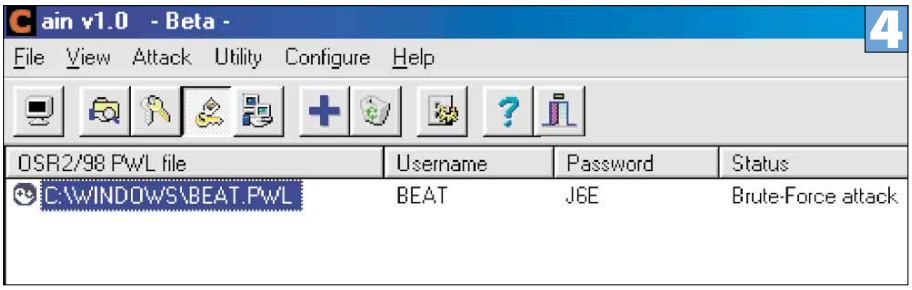
Die PIN-Nummer einer Kreditkarte besteht oft nur aus vier Zahlen. Insgesamt kennt der Nummernblock zehn Zahlen (0 bis 9). Es gibt also 10 000 mögliche Passwörter:
$10^4 = 10 \times 10 \times 10 \times 10 = 10\,000$
Sie meinen, das seien doch recht viele Möglichkeiten? Ein Rechner mit einem 2-GHz-Pentium-4-Prozessor generiert mit einem geeigneten Programm dreieinhalb Millionen Schlüssel pro Sekunde. Dividiert man die Anzahl Möglichkeiten durch die Anzahl generierter Schlüssel pro Sekunde, erhält man die Zeit, die der Computer braucht, um ein solches Passwort zu knacken. Um das richtige Passwort zu finden, dauert es in unserem Beispiel also gerade mal drei Tausendstelsekunden:
10 000 : 3 500 000 = 0,003
Natürlich wissen das auch die Verantwortlichen bei den Banken. Deshalb wird die Kontokarte nach dem dritten fehlgeschlagenen Versuch eingezogen. Immerhin besteht dank der drei Versuche noch eine Chance von 3333 : 1, den PIN-Code zu knacken.

Oft bestehen Passwörter aus Gross- und Kleinbuchstaben. Es stehen so 52 verschiedene Zeichen zur Verfügung. Gehen wir von einem achtstelligen Passwort aus, ergeben sich also 53 459 728 531 456 mögliche Kombinationen:
$52^8 = 53\,459\,728\,531\,456$
Auch hier ist die maximale Dauer einer Attacke berechenbar:
53 459 728 531 456 : 3 500 000 = 15 274 208 Sekunden = 177 Tage.

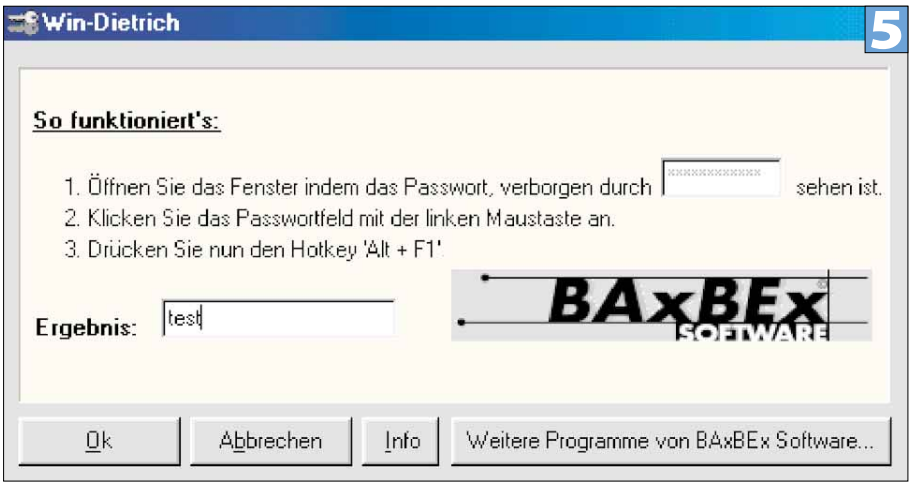
Wähnen Sie sich schon in Sicherheit? Dann haben Sie sich zu früh gefreut. Der aktuelle Duden umfasst 120 000 Stichwörter. Passwortnutzer neigen dazu, sich Wortkombinationen zu merken und nicht sinnlose Buchstabenfolgen. Deshalb probieren Hacker nicht die mehr als 53 Billionen Möglichkeiten durch, sondern verknüpfen den Passwortgenerator mit einem Wörterbuch. Das Programm probiert nur noch Wörter und Wortkombinationen aus. Deshalb dauert auch das Knacken von achtstelligen Passwörtern oft nur knapp eine Minute. Zusätzlich zum Wörterbuch suchen Hacker auch nach gängigen Tastenkombinationen wie «12345678» oder «asdfghj». Es nützt nichts, Wörter rückwärts zu schreiben («retröW»), denn auch diesen Trick kennen die Hacker.

Daraus lässt sich eine Richtlinie für Passwörter ableiten. Als sicher gelten Passwörter, die
- mindestens acht Zeichen lang sind,
- keine bekannten Wörter enthalten,
- keine gängigen Tastenkombinationen enthalten,
- sich aus Klein- und Grossbuchstaben sowie Zahlen zusammensetzen. (Falls es der Dienstanbieter zulässt, verwenden Sie auch Satz- und Sonderzeichen!)

Passwörter



Cain ermittelt die Windows-Passwörter.



Win-Dietrich übersetzt Passwort-Sternchen in Klartext.

Lösung: Eine einfache Möglichkeit, Passwörter zu knacken, ist die so genannte Brute-Force-Attacke: Ein Programm probiert automatisch jede mögliche Passwortkombination aus, bis die richtige gefunden ist. Meist fangen sie mit «A» an und hören mit «ZZZZZZZZ...» auf.

Auf der PCtip-Webseite finden Sie das Programm Cain (**http://www.pctip.ch/downloads/dl/22211.asp**). Es ermittelt verlorene Passwörter mit dieser Brute-Force-Methode, **Screen 4**.

Achtung: Verschiedene Virenschutz-Programme identifizieren Cain beim Download als einen Trojaner. Keine Angst: Die Software auf der PCtip-Homepage ist garantiert virenfrei. Aber die Programme erkennen den aggressiven Charakter des Programms und stufen es darum als Schädling ein.

Ähnliche Programme gibt es für fast jede per Passwort geschützte Software. Sie erlauben entweder das Auffinden von Passwortdateien, Brute-Force-Attacken oder schlicht und einfach das Umgehen von Passwortabfragen. Auf solche Programme spezialisiert hat sich die in Moskau ansässige Firma ElcomSoft (**http://www.elcomsoft.com/**). Im Juli 2001 kam die Firma weltweit in die Schlagzeilen, als einer ihrer Entwickler während einer Hackerkonferenz in Las Vegas vom FBI verhaftet wurde. Das wirft ein Licht auf die Probleme mit dieser Art Software: Während es legitim ist, sie für das Auffinden des eigenen Passwortes zu benutzen, ist jeder andere Einsatz illegal.

Szenario: Verborgene Passwörter

Es gibt einige Passwörter, die Sie einmal eingeben und dann speichern, z. B. wenn Sie Ihr E-Mail-Programm in Outlook einrichten. Wenn Sie später die Benutzerdaten nachschauen möchten, sehen Sie nur noch die Sternchen (******), haben aber keine Ahnung mehr, was sich dahinter versteckt.

Lösung: Es gibt Programme, die im Klartext schreiben, was sich hinter den Sternchen verbirgt. Eines davon ist die Freeware Win-Dietrich (**http://www.pctip.ch/downloads/dl/14439.asp**). Öffnen Sie Win-Dietrich und anschliessend das Fenster, in dem das Passwort als Sternchen angezeigt wird. Drücken Sie die Tastenkombination *Alt+F1*, sehen Sie das Passwort, **Screen 5**.

Die Zukunft

Auch mit Hilfe der vorgestellten Strategien bleibt die Verwendung von Passwörtern umständlich. Viele User benutzen unsichere Passwörter und setzen oft dasselbe für verschiedene Dienste ein. Ein Ansatz, diesen Missstand zu beheben, ist die Einführung von digitalen Identitäten, die für mehrere Dienste eingesetzt werden, zum Beispiel Passport von Microsoft. Mit diesem Dienst registriert sich ein Internetnutzer nur einmal und kann sich dann mit einer einzigen Identität für mehrere Dienste anmelden. Er muss sich für die verschiedensten Angebote nur noch ein Passwort merken.

Ein anderer Ansatz sind zusätzliche Geräte, die mit Hilfe biometrischer Merkmale einen Benutzer eindeutig identifizieren, zum Beispiel über einen Fingerabdruck oder die Iris des Auges. Hier entfällt ein Passwort ganz. Doch bis sich diese Systeme durchgesetzt haben, wird es noch eine Weile dauern. Bis dahin müssen Sie wohl nach wie vor Tag für Tag in den ersten Morgenstunden Ihre sechs Passwörter eingeben.