Sechs Richtige

Mit kleinen Geräten im Format eines Schlüsselanhängers können Firmen sensible Daten besser schützen.

Herkömmliche Passwörter stellen für Axel Dunkel keine ernstzunehmende Hürde dar: Wenn ein Unternehmen wissen will, wie gut seine Zugangscodes sind, dann beauftragen sie den Hattersheimer Sicherheitsexperten. Mit Know-how und verbreiteten Hacker-Programmen rückt Dunkel den Passwörtern der Mitarbeiter zu Leibe. »Das geht im Handumdrehen. Bei einem Kunden haben wir von 700 Passwörtern mehr als die Hälfte in einer Minute geknackt«, sagt Dunkel stolz.

»Passwörter, die sich ein User ausdenkt, sind in den allermeisten Fällen schlecht«, bestätigt Lars Weiler, Sprecher des Chaos Computer Clubs. Spätestens wenn Außendienstler und externe Mitarbeiter aus der Ferne via Internet auf Firmen-Computer zugreifen, sollten Firmenchefs daher für zusätzliche Schutzmechanismen sorgen. Bei größeren Unternehmen haben sich dafür so genannte Security Token durchgesetzt: eine Art elektronischer Schlüssel, der am Schlüsselbund getragen wird. Neue Anbieter, sinkende Preise und attraktive Mietofferten machen diesen Sicherheitsmechnismus jetzt auch für kleinere Unternehmen interessant.

Schlauer Schlüsselanhänger: Im Minutenrhythmus erzeugt der sogenannte Token sichere Passwörter.

Funktionsweise: Das kleine Gerät fügt dem üblichen Passwortverfahren einen zusätzlichen Einmal-Code hinzu. Dafür zeigt der kleine Schlüsselanhänger alle 60 Sekunden ein neues Passwort in Form eines Zahlencodes auf dem Display an. Diesen erzeugt es nach einem geheimen Algorithmus

Digitale Schlüssel für die Firmenserver

Ein Sicherheitssystem besteht aus zwei Teilen: der so genannte Token erzeugt das Einmalpasswort für den Nutzer, ein Serverprogramm im Hintergrund checkt die eingegebenen Daten und gewährt anschließend den Datenzugriff.

	SECUREID	ETOKEN NG-OTP	SECOVID	ACTIVCARD TOKEN
Hersteller	RSA Security	Aladdin Knowledge Systems	KOBIL Systems GmbH	ActivCard, Inc.
	www.rsasecurity.de	www.aladdin.de	ww.kobil.de	www.activcard.de
Beschreibung	Die Tokens des Marktführers erzeugen alle 60 Sekunden einen Schlüssel. Sie können nicht geöffnet werden und verfallen nach einem fest eingestellten Zeitraum von einem bis zu fünf Jahren.	Das Token erzeugt neue Passwörter auf Knopfdruck. Es zeigt die Passwörter zum Abtippen in einem eigenen Display, lässt sich aber auch in die USB-Buchse eines Computers stecken.	Die Batterie des Tokens lässt sich wechseln, die Laufzeit ist unbegrenzt. Erzeugt Passwörter auf Knopfdruck. Auch PDAs und Handys können per Software als Tokens benutzt werden.	Das Token ist durch eine PIN geschützt, die auf einer kleinen Tastatur eingegeben wird. Erzeugt Passwörter auf Knopfdruck. Ein kostenloses Testmuster kann angefordert werden.
Preis	1800 Euro für zehn Nutzer und drei Jahre Nutzungszeit	Token 75 Euro, Server für bis zu 100 Benutzer: 3500 Euro	Server und Tokens für 20 Benutzer: 2900 Euro	Server und Tokens für 25 Benutzer: 3000 Euro
FAZIT	**Verbreitete Lösung mit gutem Support durch Systemhäuser. Günstige Mietangebote im Markt.**	**Vielseitig: eignet sich für Einmal-Passwörter und auch für digitale Signaturen. Teuer.**	**Günstiges Alternativprodukt zu den US-Angeboten. Nicht zur Technologie von RSA kompatibel.**	**Zusätzliche Sicherheitssperre durch Pin-Code auf dem Token. Komplizierter in der Bedienung.**

Quelle: xxxxx. ©impulse xx/200x

Fotos: xxx

aus Parametern wie der Seriennummer des Tokens und beispielsweise der Uhrzeit. Diese Kombination muss der Nutzer zusätzlich zum Einlog-Namen und seinem klassischen Passwort während der Anmeldeprozedur am Bildschirm eintippen – vergleichbar mit dem Tan-Verfahren beim Homebanking. Auf der anderen Seite checkt ein spezielles Computerprogramm, ob Name, Passwort und aktueller Zahlencode zusammenpassen – und gewährt nur dann Zugang. »Zum Einloggen muss der Nutzer also nicht nur etwas wissen, sondern auch etwas in den Händen halten«, umschreibt IT-Experte Dunkel das Verfahren.

Das hat Alexander Rank überzeugt. Der IT-Chef des Münchner Reisebüros Travel Overland GmbH hat seine dreizehn Außendienst-Kollegen mit SecurID-Tokens von Marktführer RSA-Security versehen. »Ohne diesen digitalen Schlüssel kommt niemand von außen auf unsere Server«, sagt Rank. Statt die Tokens und die benötigte Software zu kaufen, hat Rank das gesamte System gemietet. Ein Provider betreibt die Technik gegen eine monatliche Gebühr. So offeriert beispielsweise die Stuttgarter Firma Indevis (www.indevis.de) die kleinen Geräte für eine Gebühr ab neun Euro monatlich.

Mehr passive Sicherheit

Weiterer Vorteil der digitalen Schlüssel: »Sie schulen das Sicherheitsbewusstsein der Mitarbeiter«, sagt Thomas Heinrich, IT-Leiter der Dreieicher Biotest AG. Ein Grund, weshalb Heinrich die externen Mitarbeiter des mittelständischen Pharmaunternehmens mit Token ausgestattet hat. So notieren viele Menschen ihre Passwörter auf Zettel oder lassen sie sich von geschickten Computerganoven beispielsweise über fingierte E-Mails abschwatzen. Heinrich: »Mit den Tokens dagegen ist es wie mit dem Hausschlüssel – den rückt auch niemand so einfach heraus.«

Achim Wagenknecht *ressort.computer@impulse.de*

[x] WEITERE INFOS

Knackprogramme zum Prüfen eigener Passwörter und Hintergrund-Informationen unter www.impulse.de/tokens.

Alles sicher?

Auch ohne Tokens sollten Sie Passwort-Knackern das Leben erschweren. Lesen Sie hier, wie das geht.

LANGE ZEICHENFOLGEN

Länge zählt: Für jedes zusätzliche Zeichen braucht ein Angreifer ungefähr hundert mal mehr Rechenzeit um das Passwort zu knacken. Ab acht Zeichen gelten Passwörter heute als sicher.

WÖRTER VERMEIDEN

Ein sicheres Passwort darf in keinem Wörterbuch vorkommen. Denn aktuelle Hackerprogramme probieren komplette Wörterbücher der wichtigsten Sprachen vollautomatisch durch.

ZEICHEN EINBAUEN

Sichere Passwörter enthalten auch Zahlen und Sonderzeichen. Benutzer sollten einzelne Buchstaben durch ähnliche Zeichen ersetzen. Beispiel: den Buchstaben a durch das @-Zeichen. Oder das I durch die Ziffer 1.

SÄTZE NUTZEN

Ein gutes Passwort, das man sich trotzdem einfach merken kann, erzeugt man einfach aus den Anfangsbuchstaben und Satzzeichen eines Satzes. Gut geeignet sind Liedzeilen.

PASSWÖRTER TESTEN

Wer mag, kann die Sicherheit seiner Passwort-Kreationen im Handumdrehen überprüfen. Entsprechende Knackprogramme gibt es kostenlos im Internet (siehe »Weitere Infos«).

REGELMÄSSIG TAUSCHEN

Je länger ein Passwort in Gebrauch ist, desto größer wird die Gefahr, dass es jemand herausfindet - insbesondere, wenn es für mehrere Anwendungen gilt. Sicherheitsbewusste PC-Nutzer wechseln Passwörter regelmäßig.

RICHTIG AUFBEWAHREN

Spezialprogramme wie beispielsweise Secret-SoftwareXX verschlüsseln eine Reihe von Zugangsdaten, um sie anschließend passwortgesichert beispielsweise auf handlichen USB-Sticks zu speichern. Vorteil: Der Nutzer muss sich für den Zugriff nur ein einziges Passwort merken.