Tipps & Tricks für sichere Passwörter

Datum: 14.10.2015 | Artikel 2015

Die Erstellung eines starken Passworts fällt vielen Nutzern von Rechnern und mobilen Geräten oftmals schwer. Die meisten Menschen können sich kaum ohne Probleme den vierstelligen PIN ihrer EC-Karte merken. In dem Sinne scheint es für den Großteil der User fast unmöglich, sich ein langes und kryptisches Kennwort einzuprägen, beispielsweise für die Anmeldung bei ihrem Online-Banking- oder eBay-Account oder bei Sozialen Netzwerken. Unterm Strich besitzt man schnell fünf bis zehn unterschiedliche Konten, auf die der Einfachheit halber immer mit demselben Passwort zugegriffen wird. In dem folgenden Artikel geben wir Hilfestellung, Tipps und Tricks zu starken Passwörtern.

Das häufigste und größte Sicherheitsrisiko im Umgang mit Informationstechnologie stellen weiterhin schwache Passwörter dar, die Cyberkriminelle mithilfe so genannter Brute-Force-Angriffe leicht erraten oder knacken können. Die Folge sind Datenmissbrauch und Identitätsdiebstahl. Laut einer Umfrage von Microsoft könnte letzteres in Verbindung mit Phishing einen jährlichen Schaden von rund fünf Milliarden US-Dollar verursachen. Mit dem finanziellen geht oftmals auch ein Imageverlust einher. Umso entscheidender ist die Verwendung eines starken Passworts, das ohne viel Aufwand wie folgt erstellt werden kann.

Hilfestellung für starke Passwörter

- Das Kennwort sollte aus mindestens 12 Zeichen bestehen. Im Vergleich dazu benötigt eine sichere WLAN-Verbindung nicht weniger als 20 Zeichen.
- Die Zeichenkette sollte Groß- und Kleinbuchstaben, Ziffern (0-9) und Sonderzeichen (!?%&) enthalten.
- Wörter aus Wörterbüchern, Namen von Familienmitgliedern, Haustieren oder Freunden und Bekannten sollten vermieden werden.
- Die Verwendung von Buchstabenfolgen auf Tastaturen (asdfghjkl) ist nicht empfehlenswert.
- Umlaute sind im Ausland problematisch, weswegen auf sie verzichtet werden sollte.

Wie merke ich mir ein starkes Passwort?

Häufig wird der Nutzerkomfort über die Sicherheit gestellt. So entstehen meist einprägsame, aber leicht knackbare Kennwörter. Doch die Erstellung eines sicheren, starken Passworts ist kein Hexenwerk. Ein Masterpasswort bildet die Grundlage, beispielweise aus den Anfangsbuchstaben von Wörtern eines Satzes wie: „*Im Sommer gibt es viele heiße Tage*“. Das daraus abgeleitete ***ISgevhT*** enthält zwar schon Groß- und Kleinbuchstaben, aber keine Ziffern oder Sonderzeichen und ist darüber hinaus immer noch zu kurz. Das Anfügen eines bestimmten Zusatzes, der etwa mit einem Merkmal der Webseite verknüpft ist, auf der man sich einloggen will, erhöht den Sicherheitslevel. Nimmt man Twitter als Beispiel und die Farbe des Logos als spezifischen Zusatz, ergibt sich *hellblau*. Ergänzt man die Farbe mit der Ziffer, die der Zeichenlänge entspricht (Twitter = 7 Zeichen), entsteht *hellblau07*. Verkettet man anschließend Farbe und Ziffer mit dem Sonderzeichen Raute, resultiert daraus: *hellblau#07*. Das Masterpasswort und der Zusatz werden zu guter Letzt durch Sternchen getrennt und eingerahmt. Das fertige, starke Passwort lautet: ****ISgevhT*hellblau#07*.***

Tipps zum Umgang mit Passwörtern

Besonders beim Online-Banking ist eine verschlüsselte Datenübertragung das A und O. Eine „abhörsichere“ Verbindung mit moderner SSL/TLS-Verschlüsselung erkennt der Nutzer am HTTPS oder Vorhängeschloss am Anfang einer URL. Eingegebene Daten – wie auch das Passwort – können so durch Dritte nicht abgefangen oder missbraucht werden.

Generell ist es nicht ratsam, Passwörter zu notieren, sie via E-Mail oder Instant-Messenger zu versenden oder auf dem Computer ohne eine spezielle, sichere Software zu speichern. Die Eingabe des Passworts sollte genauso geheim erfolgen wie die Eingabe des PINs am Bankautomaten.

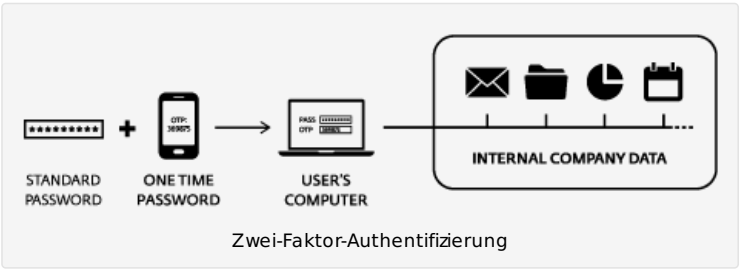
Passwörter regelmäßig ändern

Nutzern wird empfohlen, ihre Passwörter alle drei bis sechs Monate zu ändern, insbesondere bei Online-Konten wie Internet-Banking, Amazon oder Pay Pal. Wie auch beim E-Mail-Konto gilt es, die Zugänge und damit Zugriffe auf vertrauliche Daten abzusichern. Über E-Mails erfolgt die Kommunikation zu verschiedenen Diensten, bei denen ein Benutzerkonto erforderlich ist. Vergisst ein User sein Passwort, lässt es sich mit Hilfe des persönlichen E-Mail-Kontos zurücksetzen. Und auch hier lauert die Gefahr: Hat ein Angreifer Zugang zu einem E-Mail-Account, ist es ein Leichtes, ein neues Passwort anzufordern und das Konto zu kapern.

Nach Anmeldung über ein öffentliches WLAN sollte das Passwort umgehend geändert werden. Mit Hilfe von Spoofing lassen sich übertragene Daten vom Laptop zum Accesspoint abfangen und später für kriminelle Zwecke missbrauchen.

Alternativen zum Passwort

Mit einer mobilbasierten Zwei-Faktor-Authentifizierung lassen sich Sicherheitsrisiken bei der Anmeldung auf ein Minimum begrenzen, denn neben dem Passwort muss der Nutzer ein zusätzliches Einmal-Passwort eingeben. Dieser Code wird auf sein Smartphone gesendet und stellt sicher, dass sich nur berechtigte User einloggen können.



Zwei-Faktor-Authentifizierung

Personalisierte USB-Schlüssel sind eine weitere Alternative, befinden sich aber noch im Entwicklungsstatus. Alle verwendeten Passwörter sind darauf gespeichert. Nach Einstecken dieses „Masterkeys“ erfolgt die Anmeldung automatisch. Der Nutzer hätte seine verschiedenen Passwörter stets griffbereit, läuft aber auch Gefahr, den Datenträger und damit alle Kennwörter zu verlieren.

Das sogenannte, noch nicht marktreife, Nymi-Armband könnte in Zukunft per NFC-Kommunikation und Herzschlag, der bei jedem Menschen einzigartig ist, das Passwort ersetzen. Biometrische Authentifizierungsverfahren mittels Fingerabdruck- oder Iris-Scanner stehen derweil hoch im Kurs. Hinzu kommen Apps, die vor der Benutzung die Ohrform per Frontkamera „abtasten“ und erst nach Bestätigung das Gerät entsperren. Weitere Überlegungen gehen in Richtung Messung des Ganges, der Tippgeschwindigkeit oder kompletter Gesichtserkennung.

Auch die Verifizierung über virtuelle Token für Laptop-Nutzer in Verbindung mit dem Smartphone ist eine Möglichkeit. Bei der Anmeldung erscheint ein Token, beispielsweise in Form eines QR-Codes, auf dem Bildschirm und wird per Smartphone anschließend eingescannt.

Im Moment sind die Alternativen zum Passwort rar gesät. Es bleibt abzuwarten, welche Authentifizierungsmethoden sich in Zukunft durchsetzen werden, ohne Sicherheitsrisiken eingehen zu müssen. Ein starkes Passwort in Kombination mit einer Zwei-Faktor-Authentifizierung bietet derzeit den höchsten Schutzlevel und sollte von daher besonders in Unternehmen zum Standard gehören.

Intrografik: © wrangler – Fotolia.com

28 Bewertungen
Ø 4,00

Tags: PASSWORT