PASSWÖRTER: SICHER IST OFT NICHT SICHER GENUG

Veröffentlicht am 4. März 2014 von Rüdiger

Auch wenn Ihr E-Mail-Konto noch nie gehackt wurde, ist das kein Grund sich entspannt zurückzulehnen. Denn Hacker probieren einfach unzählige Passwörter aus, um ein Konto zu knacken. Wie schützt man sich nur vor den neuen Methoden der Datendiebe? Wir geben ein paar Tipps.

TIPPS FÜR IHRE PASSWÖRTER:

Die professionellen Passwort-Hacker testen Unmengen an möglichen Passwörtern. Spezielle Programme sollen imstande sein, acht Millionen Schlüsselwörter pro Sekunde durchlaufen zu lassen. Die Cyber-Kriminellen versuchen ihr Glück dabei zunächst mit den **beliebtesten Passwörtern**. Wenn also viele andere Nutzer einem bestimmten Codewort vertrauen, sollten Sie es **nicht tun**. Sogar auf Abwandlungen dieser Passwörter mit ähnlichen Zeichen (z. B. @ für a) oder Ergänzungen haben sich die Profi-Hacker eingestellt.

Grundsätzlich gilt: Was Sie sich gut merken können, ist nicht sicher. Es sei denn Sie prägen sich einen ganzen Satz ein: Nach dem sogenannten **Schneier-Schema** denken Sie sich einen Satz aus und nehmen den ersten Buchstaben eines jeden Wortes. Die **Anfangsbuchstaben** fügen Sie nun zu einem neuen Wort, Ihrem **Passwort**, zusammen. Wie sonst auch, erhöht hier die Verwendung von Sonderzeichen und Zahlen die Sicherheit des Kennworts.

Egal für welches Wort Sie sich entscheiden, sollten Sie folgende Sicherheitsmaßnahmen ergreifen:

- **Immer neu:** Für mehrere Konten dürfen Sie **nie dasselbe Passwort** benutzen. Wählen Sie für jeden Zweck ein anderes.
- **Veränderung tut gut:** Ein **Passwort** schützt Sie nur eine gewisse Zeit lang. Hin und wieder müssen Sie es **ändern** oder durch ein neues ersetzen.
- **Management:** Für die Verwaltung Ihrer Passwörter sollten Sie einen **Passwortmanager nutzen**. Unsere Media Company empfiehlt das Programm KeePass. Es ist kostenlos und umfasst auch einen praktischen Passwort-Generator.
- **Doppelter Schutz:** Wenn eine Webpräsenz eine **Zwei-Faktor-Authentifizierung** anbietet, sollten Sie sie nutzen. Diese Sicherheitsbarriere erfordert zwei Nachweise Ihrer Identität. Das heißt, dass Sie zusätzlich zum Passwort beispielsweise einen auf ihr Handy gesendeten Sicherheitscode benötigen. Seit kurzem können Apple-Nutzer zum Beispiel ihr Benutzerkonto mit der zweifachen Bestätigung sicherer machen. Nach der Aktivierung wird dem User bei jedem Einloggen ein Code auf das iOS-Gerät (iPhone, iPad) geschickt. Nur mit diesem Sicherheitscode und dem Passwort ist ein Zugang zum Konto möglich.

Unsere **Media Company** versucht, seine Partnerunternehmen bestmöglich vor Cyber-Spionage zu schützen. Dazu gehört die Nutzung und Erneuerung von sicheren Passwörtern. Damit Sie auch in Zukunft nicht von Hackern heimgesucht werden, halten wir uns in puncto **Sicherheitstechnik** stets auf dem Laufenden. Sprechen Sie uns an, wenn Sie eine Frage zu zeitgemäßem Datenschutz haben.
