Der besondere Tipp

Das sichere Passwort

Wer im Internet unterwegs ist, braucht Passwörter. Und zwar nicht nur eins, sondern viele. Zum Sichern des E-Mail-Programms, für Ebay, für Amazon, für diverse Foren, fürs Online-Banking. Und einer der größten Fehler besteht darin, für alle Anwendungen den identischen Code zu nutzen. Dann lautet das Motto: Kennst du eins, kennst du alle. Das trifft jedoch leider oft nicht nur auf den Besitzer des Passworts zu, sondern zum Beispiel auch auf Cyberkriminelle.

Was kann passieren?

Das kann verheerende Folgen haben. Am harmlosesten erscheint noch das Szenario, dass Cyberkriminelle E-Mails von meinem Zugang aus verschicken oder unter meinem Namen in sozialen Netzwerken Dinge verbreiten können. Das kann unangenehme Folgen haben. Aber wirklich schlimm wird es, wenn unter meinem Synonym teure Dinge gekauft oder ersteigert werden oder wenn der Zugang zum Onlinebanking nicht mehr sicher ist.

Schlechte Passwörter

Aber wer kann sich viele Passwörter merken? Vor allem dann, wenn sie auch noch kompliziert sind. Start1, 123456789, ABC, zyxw, das eigene Geburtsdatum, der Name des Hundes, der Geburtsort, der Lieblingsverein in der Bundesliga – das alles ist keine gute Idee, weil diese Varianten von professioneller Hacker unter Umständen in wenigen Sekunden geknackt sind. Cyberkriminelle haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen.

Worauf achten?

Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen. Das Bundesamt für Sicherheit in der Informationstechnik rät dazu, sich Passwörter möglichst nicht zu notieren, vor allem nicht in der Nähe des Computers oder gar unverschlüsselt auf der Festplatte. Stattdessen gibt es Passwort-Verwaltungsprogramme.

Außerdem sollten die Passwörter in möglichst regelmäßigen Abständen geändert werden, ein guter Richtwert ist jedes halbe Jahr. Viele Programme erinnern daran, man sollte diese Aufforderung

ernst nehmen und nicht direkt wegklicken. Bei vielen Anwendungen werden während der Installation allgemein bekannte Passwörter verwendet. Hacker wissen das natürlich.

Bei den meisten Betriebssystemen hat man die Möglichkeit, dass Bildschirm und Tastatur nach einer gewissen Zeit ohne Benutzung gesperrt werden. Das ist eine sinnvolle Möglichkeit, weil sonst unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen. Natürlich ist es ziemlich störend, wenn die Sperre schon nach kurzer Zeit erfolgt. Ein guter Richtwert ist fünf Minuten nach der letzten Benutzereingabe. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren (bei einigen Windows-Betriebssystem durch Drücken von Strg, Alt und Entf).

Ein logischer, aber oft missachteter Tipp ist auch, Passwörter niemals weiter zu geben, besonders nicht per Mail. In der Regel werden diese elektronischen Briefe unverschlüsselt versandt und können so von Dritten auf ihrem Weg durch das Internet mitgelesen werden. Zudem können E-Mails im Internet verloren gehen oder herausgefiltert werden. Der Absender einer E-Mail hat daher keine Gewissheit, dass seine Nachricht den gewünschten Empfänger auch wirklich erreicht hat. Wenn Sie ihre Passwörter an Dritte weitergeben, verlieren Sie die Kontrolle darüber und Sie haben sich umsonst die Mühe für ein gutes Passwort gemacht.

Gute Passwörter

Ein gutes Passwort sollte mindestens acht Zeichen lang sein. Dazu sollte es aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+…) bestehen. Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert. Wichtig auch: Wenn das System Umlaute wie ä, ü, ö oder ß zulässt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese eventuell nicht eingegeben werden können.

Komplizierte Passwörter leicht merken

Es gibt einen ziemlich einfachen Weg, ein kompliziertes und schwer zu knackendes Passwort zu erstellen, das man sich trotzdem merken kann. Das funktioniert mit einer Eselsbrücke, und das geht so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den ersten Buchstaben (oder nur den zweiten oder letzten, etc.). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen.

Ein Beispiel

„Morgens lese ich die Zeitung und esse dabei Müsli.“ – daraus kann man ein Beispiel für ein gutes Passwort ableiten, das gleichzeitig kompliziert und gut zu merken ist. Wenn man nur die ersten Buchstaben benutzt, entsteht daraus: „MlidZuedM.“. Das „i“ sieht aus wie eine „1“, das „und“ ersetzt man durch ein „&“. Daraus entsteht dann: „Ml1dZ&edM.“. Dieses Buchstaben und Symbolfolge ist auf dem beschriebenen Weg leicht zu merken und erfüllt alle Merkmale für ein sicheres Passwort.