Braucht mein Computer ein Passwort?

Braucht mein Computer ein Passwort?

Yvonne Steiner

Wenn Sie verhindern wollen, dass Dritte ohne Ihr Wissen auf Dateien und Programme Ihres Computers zugreifen können, dann müssen Sie Ihren Computer mit einem Passwort schützen. Ohne Passwort kann der Computer gar nicht gestartet werden. Passwörter braucht es zudem bei vielen Computeranwendungen, zum Beispiel beim Internetbanking oder wenn Sie in einem Onlineshop einkaufen. Was ist ein sicheres Passwort und wie werden all die Passwörter sinnvoll verwaltet?

Bild: Carmen Wueest

Was ist ein sicheres Passwort?

Um es gleich vorwegzunehmen: Absolute Sicherheit gibt es nicht. Durch die Beachtung einiger Regeln kann aber die Gefahr, dass Daten und Programme Ihres Computers missbraucht werden, gesenkt werden.

Sichere Passwörter enthalten Grossbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen, Umlaute und Leerzeichen. Es sollte nicht mehr als zwei gleiche Zeichen hintereinander und nicht mehr als zwei Buchstaben oder Ziffern in einer Folge hintereinander enthalten. Weder Ihr Name, Ihre Adresse noch Wörter, die im deutschen oder englischen Wörterbuch zu finden, sollten darin erkennbar sein. Die weltweit am häufigsten verwendeten schlechten Passwörter sind «Password1», «welcome» und «1234567».

Sonderzeichen geben Sicherheit

Wie erstellen Sie ein sicheres Passwort und wie können Sie es sich merken? Am besten erstellen Sie ein Passwort aus Wörtern, die Sie sich leicht merken können. Dann fügen Sie Gross- und Kleinbuchstaben, Ziffern und Symbole ein. Noch sicherer als Symbole auf der Tastatur zu verwenden sind Sonderzeichen, die durch eine Tastenkombination generiert werden: « entsteht durch die Eingabe von 174 bei gedrückter ALT-Taste; ® bei der Eingabe von 0174 auf dem Nummernblock bei gedrückter ALT-Taste.

Nehmen wir zum Beispiel das Wort «Landsgemeinde». Wenn wir jeden zweiten Buchstaben durch andere Zeichen ersetzt, entsteht beispielsweise: L1nBs e@e/n£e. Wenn die Reihenfolge dieser anderen Zeichen für Sie

einen Sinn ergibt, dann umso besser. Denn so können Sie sich das Passwort merken. Aufschreiben sollten Sie Ihre Passwörter nämlich nicht. Das erhöht das Sicherheitsrisiko, besonders dann, wenn Sie die Liste Ihrer Passwörter unter die Schreibtischunterlage legen …

Vorsicht beim Passwortcheck

Ob und wie sicher Ihr Passwort ist, können Sie im Internet überprüfen, zum Beispiel auf www.passwortcheck.ch, der Seite des Datenschutzbeauftragten des Kantons Zürich. Hier wird angegeben, ob ein Passwort schwach oder stark ist. Das Passwort L1n-Bs e@e/n£e wird als stark bezeichnet. Bei 2 Milliarden Tests pro Sekunde bräuchte ein Computer über 1 Milliarde Jahre, bis er alle 12 Zeichen in die richtige Reihenfolge gestellt und somit das Passwort geknackt hätte. Aber aufgepasst, das ist eine Wahrscheinlichkeitsrechnung. Das heisst, dass der Computer über eine Milliarde Jahre braucht, bis er alle möglichen Kombinationen mit den zwölf Zeichen durchprobiert hat. Die richtige Kombination kann er theoretisch aber auch schon nach zehn Sekunden finden …

Und noch ein Tipp: Sind Sie vorsichtig mit den Tausenden von Passwortcheckern im Internet. Geben Sie nie Ihr richtiges Passwort ein, sondern machen Sie nur Eingaben, deren Aufbau und Struktur Ihrem echten Passwort ähnlich sind. Geben Sie nämlich Ihr echtes Passwort ein, wissen Sie wohl nachher, wie stark es ist, aber Sie wissen nicht, ob es nun schon in falschen Händen ist!

Passwort nur einmal verwenden

Für den sicheren Umgang mit Passwörtern sollte man sich im eigenen Interesse an folgende Regeln halten: Für verschiedene Accounts nie das gleiche Passwort verwenden; wenn ein Zugang ein neues Passwort fordert, machen Sie sich die Mühe, ein ganz anderes zu erstellen. Passwörter nie auf der Festplatte speichern; dort können sie von Trojanern oder anderen Benutzern ihres PC ausgespäht werden. Wenn Sie Passwörter aufschreiben, halten Sie diese Liste unter Verschluss und machen Sie sie nur einer vertrauten Person oder Ihrem Anwalt zugänglich; das ist vor allem auch im Hinblick auf das eigene Ableben zu berücksichtigen.

Mehr Sicherheit mit dem Passwort-Manager

Wer sich im Internet bewegt und die Regel befolgt, ein Passwort nicht mehrfach zu verwenden, der hat es bald einmal mit einem guten Dutzend Passwörter zu tun. Sich diese alle zu merken, geht nicht, sie aufzuschreiben, ist eine schlechte Lösung. Da bieten Kennwortverwaltungsprogramme (Passwort-Manager) Hilfe an. Mit diesen Computerprogrammen können die Benutzer Kennwörter verschlüsselt speichern, verwalten und in der Regel auch sichere Kennwörter erzeugen. Die Passwort-Software merkt sich alle Zugangsdaten des Nutzers und hat diese bei Bedarf sofort parat. Dafür braucht sich der Nutzer nur ein einziges Masterpasswort zu merken. Man kann sich das Programm wie einen Passwort-Tresor vorstellen. Darin sind alle Zugangsdaten sicher hinterlegt, der Zugriff erfolgt über ein einziges Passwort.

Haben Sie Bedenken, Ihre sämtlichen Zugänge einer einzigen Anwendung anzuvertrauen? Solche Bedenken gelten heute als unbegründet. Mittels moderner Verschlüsselungstechniken werden Ihre Daten unknackbar lokal auf dem eigenen Endgerät gespeichert. Das Masterpasswort kann geheimgehalten werden und muss nirgendwo im Internet angegeben werden. Gängige Passwort-Manager für Windows sind Password Depot, Steganos Passwort Manager oder Kaspersky Password Manager. Bekannte Produkte für Mac heissen 1Password und mSecure Password Manager. Die von fast allen Webbrowsern angebotenen Möglichkeiten zur Kennwortspeicherung werden hingegen als unsicher bewertet.