Passwörter merken leicht gemacht

Wer kennt sie nicht, die vielen Richtlinien und Hinweise zur Auswahl eines sicheren Passwortes? Mindestens 8 Stellen, Groß- und Kleinschreibung, Ziffern und dann bitte auch noch Sonderzeichen – aber ja nicht aufschreiben! Doch was nützt das sicherste Passwort, wenn man es sich nicht merken kann?

Der Konflikt um ein sicheres Passwort beschäftigt heute fast jeden Internetnutzer: mindestens eine Email-Adresse, Onlinebanking, Ebay, dazu noch eine Online Community und ein Instant Messenger – man geht davon aus, das ein Internet Nutzer durchschnittlich etwa zehn Passwörter benötigt. Sich zehn verschiedene und voneinander unabhängige Passwörter zu merken, die alle den nötigen Sicherheitsanforderungen genügen, überfordert jedoch die meisten Nutzer. Daher greifen diese auf einfachere Passwörter zurück, benutzen immer ein und dasselbe Passwort oder setzen Passwort-Tools ein, in denen sich alle genutzten Passwörter befinden und bei Bedarf abgerufen werden können. All diese Varianten bergen jedoch große Sicherheitsrisiken:

Passwörter wie z.B. der Name des Partners mögen zwar leicht zu merken sein, bieten aber so gut wie keinen Schutz, da sie durch einfache Wörterbuchangriffe oder sogar nur durch einen informierten Angreifer geknackt werden können. Benutzt man bei allen Gelegenheiten das gleiche Passwort, so ist es mit Hilfe von gezielten Hacker-Angriffen möglich, sich Zugang zu weiteren Accounts zu verschaffen, sobald nur ein einziger Zugang geknackt wurde. Auch Passwort-Tools stellen keine zufriedenstellende Lösung dar, da sie extrem unsicher sind, sobald ein Angreifer Zugang zum System hat.

Doch es gibt eine Lösung, die es möglich macht, beliebig viele sichere Passwörter zu erhalten ohne sich auch nur eines davon vollständig merken zu müssen: das algorithmierte Passwort. Bei dieser Methode denkt sich der Nutzer einen festen Algorithmus (also eine Herleitungsregel) aus, den niemand außer ihm kennt und nach dem er für jeden Internetdienst sein Passwort herleiten kann. Je nach Schwierigkeitsgrad bzw. Komplexität des Algorithmus ist das generierte Passwort mehr oder weniger sicher. Um die Vorgehensweise zu verdeutlichen hier ein Beispiel, wie ein Algorithmus aussehen könnte:

Das Ziel soll sein, ein Passwort zu erhalten, das aus einem festen und einem generierten Teilstück besteht. Als festes Teilstück benutzen wir zum Einen „ZEDAT“ und zum Anderen „07“. Das Passwort soll schließlich folgendermaßen aufgebaut sein: „ZEDAT“+„generierter Teil“+„07“. Um den generierten Teil zu erhalten benötigen wir nun einen Algorithmus. Als Basis nehmen wir uns die Adresse des Internetdienstes, für den wir ein Passwort benötigen, z.B. www.amazon.de. Nun bauen wir die letzte Silbe als

generierten Teil in das Passwort ein und erhalten vorläufig „ZEDATzon07“. Bräuchten wir ein Passwort für www.youtube.com, würde sich bis jetzt „ZEDATtube07“ ergeben. Jetzt fügen wir dem generierten Teil noch weitere Faktoren hinzu. Wir nehmen die Anzahl der Buchstaben in der betreffenden Adresse (im Fall von www.amazon.de wäre das eine 6) und schließlich noch die Anzahl der Vokale, hier eine 3. Zusammengesetzt ergibt sich die Zahl 63. Diese fügen wir an den bisher generierten Teil unseres Passwortes an und erhalten „ZEDATzon6307“. Das gleiche Schema auf die Adresse www.youtube.com angewendet ergibt mit 7 Buchstaben und 4 Vokalen die Zahl 74, also als Passwort „ZEDATtube7407“. Diese Passwörter sind schon recht sicher, da es so bereits relativ schwer ist, beim Betrachten der Passwörter ein Schema zu erkennen. Trotzdem fällt es dem Nutzer leicht, die Passwörter zu erhalten – ohne sich diese merken zu müssen! Er muss sich einzig den Algorithmus merken, nach dem die Passwörter hergeleitet werden: „Man nehme die letzte Silbe der Internetadresse, füge die Anzahl der Buchstaben und die Anzahl der Vokale, die in der Adresse auftauchen, an und setze diesen generierten Teil zwischen „ZEDAT“ und „07“.“

Nach dieser Vorgehensweise kann das Passwort je nach Aufbau und Komplexität des Algorithmus beliebig kompliziert gestaltet werden. Denkbar wäre z.B. ein Aufbau des Passwortes, der sich aus mehreren generierten Teilen zusammensetzt („fester Teil 1“+„generierter Teil 1“+„fester Teil 2“+„generierter Teil 2“) und dazu noch Sonderzeichen enthält. Sonderzeichen lassen sich beispielsweise ermitteln, indem man wie oben eine Zahl generiert und diese dann durch die Sonderzeichen auf den entsprechenden Tasten ersetzt. Aus „734“ würde also „/§$“.

Mithilfe eines hinreichend komplexen Algorithmus dessen Faktoren man sorgfältig ausgewählt hat, ist es so also möglich, verschiedene sichere Passwörter zu erstellen. Der entscheidende Vorteil für den Anwender liegt jedoch vor allem darin, dass er sich nicht mehr dutzende verschiedener Passwörter merken muss, sondern nur einen einzigen Algorithmus, mit dessen Hilfe er sich beliebig viele sichere Passwörter herleiten kann.

Alena Kiwitt