Wie erlange ich ein sicheres Passwort?

IT-SICHERHEIT (TEIL 16) Zum Abschluss des Themenblocks »Passwörter« (Fortsetzung aus »de« 21.2017, S. 74/75), zeigt dieser Beitrag die Vorgehensweise bei der Erstellung eines guten und sicheren Passworts auf.

Keine Frage: Wer immer noch ein Passwort mit 8 Zeichen benutzt, das zum Beispiel so aussieht → »12345678«, der läuft früher oder später Gefahr, sich in den Fängen eines Angreifers aus dem Netz zu befinden. Ja, es hat auch etwas mit Selbstdisziplin zu tun, sich für jeden Zugang ein anderes Passwort auszudenken und dieses regelmäßig zu ändern. Dies wird häufig von der eigenen IT-Administration gefordert.

Verschiedene Möglichkeiten der Passwortfindung

Einen langen Satz bilden

Denke Sie an einen etwas längeren Satz wie z.B. »Wenn ich Montag zur Schule gehe, habe ich in der 1. Stunde Sport!«. Aus jedem Anfangsbuchstaben ergibt sich ein Zeichenkettenkombination, die sich als Kennwort eignet: »WiMzSghiid1SS!« (**Bild 60**).

Namen aus einer Gruppenreihenfolge

Auch lange Namen können Sie für ein Kennwort nehmen, wie der ausführliche Name von Pippi Langstrumpf: »Pippilotta Viktualia Rollgardina Schokominza Efraimstochter Langstrumpf«. Würde man nur die Anfangsbuchstaben nehmen, fehlen uns noch die Kleinbuchstaben, die 8-Zeichenlänge und ein Sonderzeichen.

Der Kreativität sind keine Grenzen gesetzt: »P1V1Ro44ScEfLa«. Das »i« wurde durch eine 1 ausgetauscht. Die Pippi-Geschichte wurde 1944 niedergeschrieben. Diese Zahl wurde in die Mitte gesetzt. Durch die Verwendung von zwei Stellen pro Silbe ist das Kennwort nun lang genug und enthält dazu Kleinbuchstaben.

Personen einer Gruppe haben sich in der Praxis ebenfalls bewährt. Stellen Sie sich vor, Sie sind Mitglied eines Tischtennisvereins. Jährlich wird durch die Vereinsmeisterschaften eine Rangfolge ausgespielt. Für den Kreis der aktiven Spieler ist dies bekannt. In unserem Beispiel (**Bild 61**) ergibt sich nun folgendes Ergebnis:

- Andreas Huber, 27 Jahre, Rang 1
- Wolfgang Becker, 20 Jahre, Rang 2
- Michael Korks-Schreiber, 35 Jahre, Rang 3 und
- Tim Mustermann, 21 Jahre, Rang 4.

Aus dieser Liste lässt sich leicht ein Kennwort kreieren wie »aH27wB20mK-S35tM21«. Die Wahrscheinlichkeit, dass jemand anderes auf das gleiche Schema kommt , dieses als Kennwort missbrauchen möchte, eine mögliche Cyber-Attacke bei der betreffenden Person starten und den betreffenden Zugangsschutz wählt ... nein, die Wahrscheinlichkeit eines möglichen Angriffs wird ad absurdum geführt. Solange die Verwendung und das Schema nicht weitergegeben werden, bleibt das Kennwort sicher. Hinzu kommt, dass sich die Rangliste jährlich ändert und damit auch die Kombination der Zeichenkette.

Verse eine Lieds oder eines Gedichts

Gedichte, Lieder, Phrasen o.ä. können sich auch für die Bildung von Kennwörtern eignen wie »Ich weiß nicht, was soll es bedeuten, dass ich so traurig bin.« Das Lied stammt von Heinrich Heine und ist unter dem Namen »Das Loreleylied« aus dem Jahr 1823 bekannt. Das Kennwort dazu könnte so aussehen: »Iwn,wseb,distb.HHDL1823«. Mit ein wenig Kreativität ist vieles möglich. Für die vielen Varianten des Kennworts sind auch Ableitungen denkbar. Letztendlich weiß der Angreifer nicht in welcher Intensität und an welchen Stellen das Kennwort abgeändert wurde. Eine Zeichenkette wie »Monster Rock 1987« könnte man in »M0nst@r R0ck 1987« ändern. Zumindest entspricht es den Richtlinien.

Ableitung bestehender Kennwörter

Gerade bei älteren Konten ist vielleicht noch ein Kennwort gewählt worden, das den aktuellen Richtlinien nicht entspricht. Kennwörter lassen sich aufbessern. Dabei können Anhängsel, Vorsilben oder Trennzeichenketten zum Einsatz kommen. Diese werden einfach vor, zwischen oder an das Kennwort gehängt.

Quelle: alle Bilder C. Strobel

Bild 60: Die Anfangsbuchstaben eines langen Satzes sind die Grundlage einer Methode für die Passwortfindung

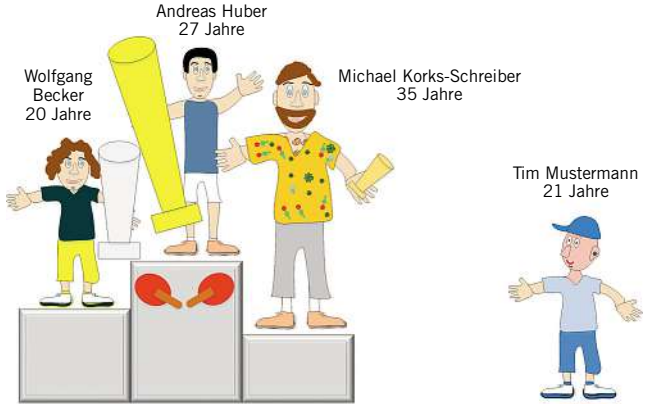

Bild 61: Aus der Rangliste eines Tischtennisvereins lassen sich ebenso sichere Passwörter bilden

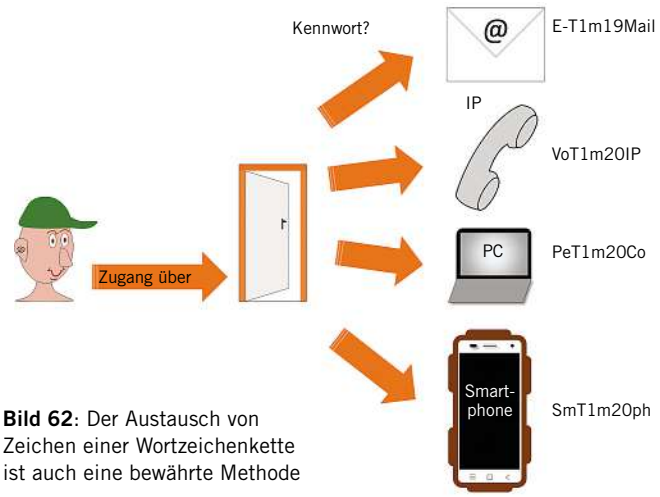

Bild 62: Der Austausch von Zeichen einer Wortzeichenkette ist auch eine bewährte Methode

Eine weitere Variante, die sich bewährt hat, ist folgende. Es lässt sich ein Symbol oder eine Zahl in eine bestehende Wortzeichenkette durch den Austausch mit einem Buchstaben integrieren. Ein mäßiges Kennwort wie »Orgel« wird dann durch die Ziffer »0« zur »Orgel« oder »März« wird durch das E-Mail-Zeichen »@« zu »M@rz«. Das lässt sich weiter miteinander kombinieren wie »M@rzOrgel«, »OrgelM@rz« oder »OrM@rzgel«. Die Kennwortrichtlinien werden damit eingehalten.

Das **Bild 62** verdeutlicht diese Vorgehensweise. Aus den folgenden Vorgaben wurden dann jeweils die Kennwörter, die am rechten Bildrand zu sehen sind:

- E-Mail – Tim – 19 Jahre
- VoIP – Tim – 20 Jahre
- Personal Computer – Tim – 20 Jahre
- Smartphone – Tim – 20 Jahre.

Passwort-Generatoren

Wir haben gesehen, dass sich Kreativität bei der Gestaltung des eigenen Kennworts lohnt. Doch wie handhaben es IT-Administratoren, die häufig keinen persönlichen Bezug zu allen Betriebsmitarbeitern haben können? Wie kommen geeignete Kennwörter zustande? Es gibt Kennwort-Generatoren, die eine zufällige Zeichenkettenfolge erstellen. Ein sehr einfaches Tool ist »PWGen« (**Bild 63**) und findet sich über die Webseite des PC-Magazins »Chip« (www.chip.de) oder unter www.sourceforge.net. Sie können sich auch direkt auf der Webseite Ihre Passwörter nach vorgegebenen Richtlinien erstellen; unter **www.pwgen.de** geht das ganz einfach. Probieren Sie es ruhig einmal aus.

Viele Kennwortgeneratoren – wie auch dieser in Bild 63 – wirken unter heutigen Voraussetzungen und Gewohnheiten sehr schlicht. Manche Betriebe haben sogar selbst geschriebene Software im Einsatz. Das ist letztendlich eine Vertrauensfrage. Bei unserem Tool lässt sich die Zusammensetzung des zu generierenden Kennworts einstellen. Über Maus-Bewegungen werden Zufallswerte ermittelt.

Wie lässt sich die in unserem Beispiel generierte Zeichenkette »]1A>]`{„kcPt« für den Endanwender in den Kopf bekommen? Sie lesen richtig: Es geht auch ohne Eselsbrücken oder persönlichen Bezug. Tippen Sie diese Kombination mehrmals ein. Irgendwann ist sie bei Ihnen im Kopf. Erst im Kurzzeitgedächtnis, später im »Langzeitspeicher«.

Priorisierung der Zugänge

Wie schafft man es als einzelne Person, sich Kennwörter für verschiedene Zugängen zu merken und dabei den Richtlinien zu entsprechen? Kreativität, Struktur und Persönlichkeit sind die Schlüssel. Je-

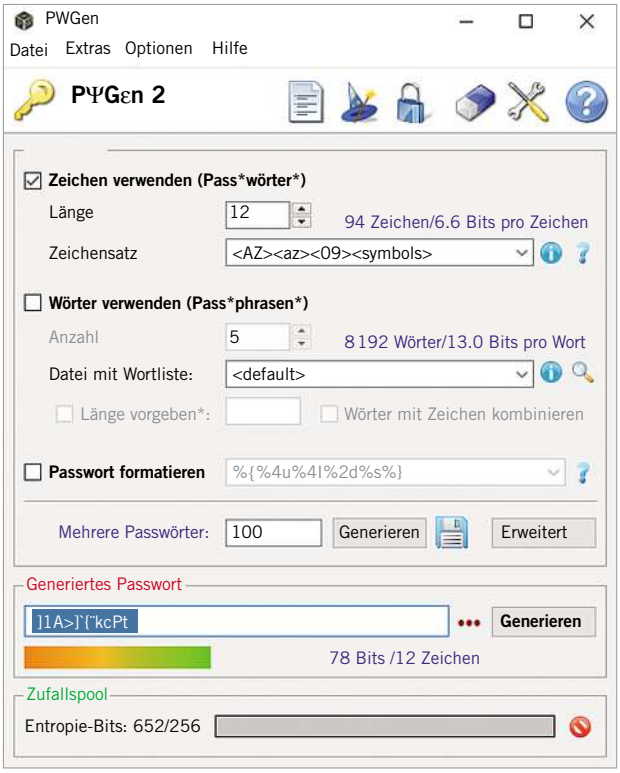

Bild 63: Bei dem Passwort-Generator »PWGen« werden über Mausbewegungen Zufallswerte ermittelt

der Zugang sollte bezüglich der Gefährdung selbst beurteilt werden. Online-Banking, E-Mail, Online-Shopping dürften als hoch eingestuft werden, während eine Anmeldung für einen Newsletter, eine Mitgliedschaft in einem Forum oder die Registrierung zum Ausprobieren einer Software eher sekundär sind.

Kennen Sie das auch? Um neue Software zum Ausprobieren herunterzuladen, muss diese vorher registriert werden, häufig kostenlos. Zur Registrierung wird die E-Mail-Adresse und ein neu zu vergebendes Kennwort erforderlich. Ist gibt damit eine Abhängigkeit, ohne E-Mail kein Software-Download. Wurde das Kennwort für den Software-Download vergessen, kann es über die E-Mail zugesandt werden. Das gilt auch für viele andere Online-Konten.

Die Zugangsdaten für den E-Mail-Account sind gegenüber dem Software-Download mit höherer Wertigkeit zu betrachten, weil ein Angreifer an die Online-Konten herankommt, falls er den Zugang zum hinterlegten E-Mail-Konto besitzt.

Wie ist es mit dem Bank-Account? Lässt er sich unabhängig einstufen? Ja, in der Regel schon. Nach persönlicher Gefährdungsbeurteilung sollte dieser ebenfalls hoch eingestuft werden.

Einen kleinen Ratgeber zu dem Thema finden Sie auf der BSI-Seite unter **https://www.bsi-fuer-buerger.de**. Der kommende Betrag befasst sich dann mit dem Thema E-Mail-Kommunikation. Worauf sollte geachtet werden? Woher kommen die Gefahren und wie verhält man sich am besten?

(Fortsetzung folgt)

AUTOR

Claus Strobel
Dozent IT/ET; Schwerpunkt Netzwerktechnik,
Elektro-Technologie-Zentrum, Stuttgart