Sicherer Umgang mit Passwörtern

Regel 1: Ihr Passwort ist sehr wichtig

Einbrecher greifen nicht nur geheime Server an, sondern jeden Rechner, den sie finden können. Es ist also auch Ihr Rechner gefährdet – selbst wenn Sie ihn nur für eine bessere Schreibmaschine halten. Dadurch kann Ihr Rechner die Sicherheit des gesamten UR-Netzes gefährden.

Regel 2: E-Mail-Postfach besonders schützen

Wer Zugriff auf Ihre E-Mails hat, hat auch Zugriff auf fast alle anderen Online-Dienste. Denn bei den meisten Diensten ist es möglich, mit nur einem Klick ein neues Passwort oder einen Passwort-Link per E-Mail zusenden zu lassen.

Regel 3: Verwenden Sie kein Passwort, das erraten werden kann

Benutzen Sie nicht die Namen Ihrer Kinder, Ihres Partners oder das Kennzeichen Ihres Autos. Diese Daten sind offensichtlich und leicht herauszufinden.

Regel 4: Kein Passwort aus einem Wörterbuch

Passwörter werden meist verschlüsselt abgespeichert. Ein Cyberkrimineller kann zwar die codierte Version stehlen, diese aber nicht ohne weiteres entschlüsseln. Er kann jedoch Wörterlisten (z.B. Wörterbücher, Wikipedia, Duden) benutzen und jedes Wort darin verschlüsseln. Dann werden die verschlüsselten Wörter mit den Passwortcodes verglichen. Stimmt ein Passwortcode mit dem Wörterbucheintrag überein, hat der Cyberkrimineller ein Passwort erraten. Computer können tausende Wörter pro Minute verschlüsseln und vergleichen. Daher dürfen Sie kein Passwort verwenden, das in einem Wörterbuch steht.

Regel 5: Lange Passwörter mit verschiedenen Zeichen

Passwörter zu erraten bzw. automatisch abzugleichen, kostet Zeit. Je länger das Passwort ist, desto höher ist der zeitliche Aufwand. Wählen Sie mindestens ein 14-stelliges Passwort aus verschiedenen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen aus. Je länger und gemischter, desto besser.

Regel 6: Passwort nicht weitergeben

Nur Sie kennen Ihr Passwort. Schreiben Sie es nicht auf und nennen Sie es keinem Drittem.

Regel 7: Das Passwort schützen

Achten Sie darauf, dass Dritte nicht auf die Tastatur schauen können, wenn Sie das Passwort eingeben. Nutzen Sie Sichtschutzfolien für Laptops. Dies gilt insbesondere für öffentliche Plätze. Dazu gehört auch, dass Sie Passwörter nur an Computern eingeben, denen Sie vertrauen können.

Regel 8: Verschiedene Passwörter

Verwenden Sie auf gar keinen Fall Ihr System oder E-Mail-Passwort an anderen Stellen. Sie wissen nie, wer z.B. hinter einem Web-Forum steht. Es kann sein, dass Ihr Passwort abgefangen oder weitergeleitet wird. Daher verwenden Sie auf jeder Webseite, in jedem Forum, für jeden E-Mail Account, also immer ein eigenes Passwort.

Regel 9: Passwörter nicht im Browser speichern

Die meisten Browser bieten die Möglichkeit, Benutzernamen und Passwörter für Webseiten zu speichern. Das ist zwar hilfreich, aber prinzipiell auch unsicher. Hat ein Angreifer Zugriff auf Ihren Rechner, kann er eventuell die gespeicherten Passwörter auslesen.