Schwache Passwörter stiften großen Schaden

Wer denkt, IT Sicherheit sei ausschließlich etwas für Computerfreaks, der hat die Zeichen der Zeit verkannt und bewegt sich mit geschlossenen Augen und übergroßen Schuhen durch ein Minenfeld. Basiswissen im Bereich Computersicherheit ist ein Muss für jeden Anwender, gleich ob Schreibkraft oder Manager.

Der Verteidigungshaushalt der Bundesrepublik Deutschland lag im Jahr 2015 bei etwa 33 Milliarden Euro. Der durch den Branchenverband ›Bitkom‹ geschätzte Schaden, der der deutschen Wirtschaft jährlich durch Spionage, Sabotage und Datendiebstahl entsteht, liegt bei sagenhaften 51 Milliarden Euro.

Die Schadensverursacher stammen in den meisten Fällen aus dem Unternehmensumfeld. Der Täterkreis setzt sich mit mehr als 50 Prozent aus aktuellen oder ehemaligen Mitarbeitern zusammen, die oft nicht in böser Absicht handeln. Unvorsichtigkeit und vor allem Unwissenheit führen zu Fehlhandlungen mit oft dramatischen Folgen. Wer möchte schon gerne dafür verantwortlich sein, dass wichtige Unternehmensdaten abfließen oder die Produktion zum Stillstand kommt? Selbst mit der besten IT-Abteilung im Rücken ist niemand davon entbunden, geeignete Maßnahmen zu ergreifen, um es potenziellen Datenräubern und Industriespionen so schwer wie möglich zu machen.

»Je sicherer sich jeder einzelne im Netz bewegt, umso besser können Staat und Gesellschaft geschützt werden.« (Thomas de Maizière; Vorwort zu Bericht des Bundesamtes für Sicherheit in der Informationstechnik aus 2015)

Es geht darum, sich als „Homo Digitalis“ angstfrei, selbstbewusst und sicher durch das 21. Jahrhundert zu bewegen. Mindestens an einer Stelle kommen wir alle mit dem Thema ›IT-Sicherheit‹ in Kontakt. Es sind Passwörter, die als eine Art „Haustürschlüssel“ den Zugang zu wichtigen Informationen, sensiblen Daten und persönlichen Diensten regeln. Sie schützen E-Mail-Konten vor nicht autorisierter Verwendung, regeln den Zugriff auf Firmennetzwerke und Server, kommen beim Online-Banking und -Shopping zum Einsatz, gestatten den Zugriff auf soziale Medien und vieles mehr. Trotz der Bedeutung des Passwortes wird nicht selten äußerst arglos damit umgegangen. Wie sonst wäre erklärbar, dass immer noch Passwörter wie ›123456‹, ›Sommer16‹ oder ›Mia22052015‹ zum Einsatz kommen? Wer würde mit einem solchen Passwort seine Haustür absichern? Die Arglosigkeit ist im Wesentlichen die Folge von Bequemlichkeit (starke Passwörter kann man sich schwer merken) und einer gestörten Wahrnehmung der eigenen Gefährdungssituation (mich wird schon keiner angreifen).

Dipl.-Ing. Patric Remus
Inhaber Softwareentwicklung Remus

Auch in Zeiten, in denen biometrische Systeme wie Fingerabdrucksensoren oder Irisscanner immer mehr den Zugang auf sicherheitsrelevante Bereiche und Daten regeln, wird uns das Passwort noch lange nicht verlassen. Ein Argument für das klassische Passwort ist unschlagbar: Die Implementierung ist einfach und äußerst günstig. Vor diesem Hintergrund ist es mehr als lohnenswert, einmal einen Blick auf die Anforderungen an ein gutes Passwort zu werfen.

Die Länge eines Passworts und der Zeichenvorrat aus dem es aufgebaut ist, sind von großer Wichtigkeit für die Sicherheit. Es gibt immer noch viele Internetseiten, die sechs Zeichen lange Passwörter als ausreichend sicher akzeptieren. Unverantwortlich! Ein gutes Passwort sollte aus mindestens 12 Zeichen bestehen. Zur Sicherung des WLANs dürfen es durchaus 20 Zeichen sein. Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen sollten einfließen. Angreifern darf keine Angriffsfläche durch leicht zu erratende Passwörter geboten werden. Passwörter mit einem starken Bezug zum persönlichen Umfeld sind zu vermeiden. Vor allem sollte nicht auf lexikalische Begriffe zurückgegriffen werden, da derart konstruierte Passwörter sogenannten ›Wörterbuchangriffen‹ nicht lange standhalten.

Wer sein Augenmerk einmal auf Begriffe wie ›Passwortdiebstahl‹ oder ›Diebstahl von Zugangsdaten‹ richtet, der wird immer wieder Meldungen finden, in denen es um die Entwendung von Nutzerdaten im großen Stil geht. Gehackte Twitterkonten, gestohlene Daten bei Badoo, Yahoo und LinkedIn sind folgenschwer. Mit speziellen Verfahren werden aus den teilweise verschlüsselten Daten die Login-Daten rekonstruiert. Solche Vorkommnisse verdeutlichen, dass man im Umgang mit Passwörtern ein paar weitere Punkte beachten muss.

Selbst die Wahl eines guten Passwortes schützt nicht grundsätzlich. Es liegt nicht immer in unserer Hand, ob ein Passwort geheim bleibt. Daraus lässt sich folgern, dass wir niemals ein Passwort an mehreren Stellen verwenden sollten. Ist ein Passwort einmal von Datendieben entwendet worden, wird versucht, damit Zugriff auf E-Mail-Konten, Cloud-Dienste, Shopping-Plattformen und soziale Medien zu bekommen. Erst wenn ein Schaden eintritt und zum Beispiel unter unserem Namen bei eBay andere Kunden betrogen werden, bemerken wir den Diebstahl.

Zugangsdaten mit weiteren Informationen zur Person werden massenhaft im so genannten ›Darknet‹ angeboten. Das Aufbereiten und Entschlüsseln dieser Daten nimmt häufig einige Zeit in Anspruch. Daher kann man durch regelmäßiges Ändern von Passwörtern verhindern, dass allzu viel Schindluder mit den Daten getrieben wird.

Sieht man sich die Tipps und Hinweise an, wird überdeutlich, dass man sich einer Kraftanstrengung gegenübersieht. Sichere Passwörter sind komplizierte Zeichenfolgen. Komplizierte Zeichenfolgen lassen sich schwer merken. Und selbst dann, wenn man ausreichend komplexe Passwörter wählt, muss man daran denken, sie regelmäßig zu ändern. Zum Glück gibt es Tools wie Passwortmanager, die viel Arbeit abnehmen und für eine deutliche Steigerung der Sicherheit beim Umgang mit Passwort- und Zugangsdaten sorgen.

archicrypt.de