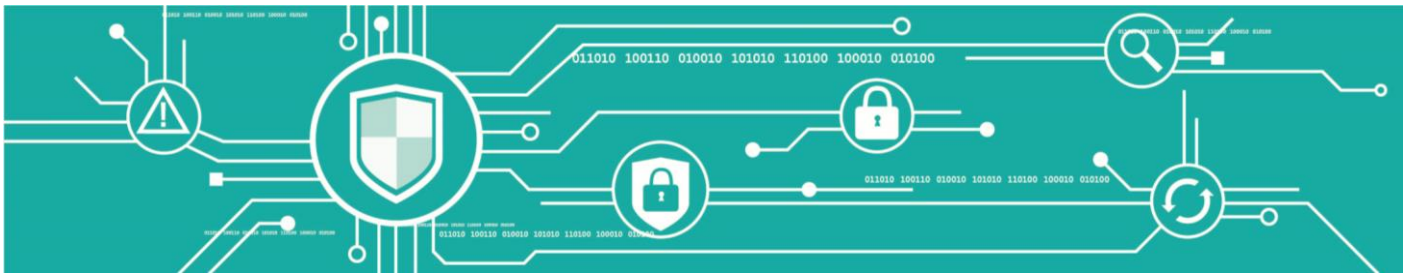

5 Passwort Mythen zum Welttag des Passwortes

Jeden ersten Donnerstag im Mai ist Welttag des Passworts. Schon seit fünf Jahren versuchen Unternehmen, mit dem Aktionstag auf Onlinesicherheit aufmerksam zu machen und Nutzer zu sensibilisieren. Trotzdem haben sich bis heute viele Mythen gehalten, was ein Kennwort wirklich schwer zu knacken macht.

Mythos 1: Passwörter brauchen möglichst viele Sonderzeichen

Ein gutes Passwort hat zwei Eigenschaften: Es ist für Angreifer schwer zu erraten und für Nutzer leicht zu merken. Kennwörter aus verschiedenen Buchstaben, Zahlen und Sonderzeichen sind zwar relativ sicher, aber schwer zu merken, etwa «(g93äZ?/». Da dasselbe Passwort nicht auf mehreren Seiten verwendet werden sollte, kann es mit solchen Passwörtern schnell unübersichtlich werden. Es gibt eine bessere Methode, die ebenfalls sehr sicher und dazu noch gut zu merken ist: lange Passwörter. Sie sind sicher, weil Kriminelle meist versuchen, Kennwörter durch das sogenannte Bruteforce-Verfahren zu knacken. Das bedeutet, sie probieren verschiedene Zeichenkombinationen systematisch durch – und zwar mehrere Millionen in der Sekunde. Jedes zusätzliche Zeichen im Kennwort erhöht die Sicherheit exponentiell. Es ist also besser, eine leicht zu merkende Passphrase, also einen «Satz», zu kreieren, als ein einzelnes Passwort. Persönliche Daten haben in einem Passwort nichts zu suchen, denn sie könnten erraten werden.

Mythos 2: Häufige Passwortwechsel erhöhen die Sicherheit

Viele Angestellte kennen das: Die IT-Abteilung hat schon mehrmals den Tausch des Passworts verlangt, aus «Sicherheitsgründen». Widerwillig haben die Mitarbeiter dann ihrem alten Passwort ein neues Ausrufezeichen hinzugefügt – schon das sechste! Aber bringt es überhaupt etwas, regelmässig neue Passwörter zu nutzen? Im Prinzip ja, wenn man komplett neue Passwörter verwendet. Aber das tun nur die wenigsten, haben Forscher der Menschen neigen dazu, ein schwächeres Passwort auszuwählen, wenn sie wissen, dass sie es ohnehin bald ändern müssen. Der Befehl aus der IT-Abteilung ist also gut gemeint, scheitert aber an den Mitarbeitern, die vor den Firmenrechnern sitzen. Der Mensch ist aus Sicht der IT-Sicherheit eine Schwachstelle. Man sollte Kennwörter lieber dann wechseln, wenn es einen Angriff gab und das Passwort gestohlen worden sein könnte. In so einem Fall sollte man schnell handeln.

Mythos 3: Die Zwei-Faktor-Authentifizierung ist kompliziert und unnötig

Ein Bankkonto ist am Geldautomaten recht einfach gesichert: Die PIN besteht nur aus sechs Zahlen. Trotzdem werden Konten nicht reihenweise leer geräumt. Das liegt an der Bankkarte. Nur Karte und PIN zusammen lassen einen Kunden Geld abheben. Wer nur eins von beiden hat, kommt nicht an das Geld. Onlinekonten lassen sich nach demselben Prinzip sichern – mit der Zwei-Faktor-Authentifizierung (2FA). Mit 2FA wird eine zweite Sicherheitsstufe etabliert. Nutzer können sich nicht mehr anmelden, wenn sie nur das Passwort kennen. Sie müssen zusätzlich einen weiteren Code eingeben, der zum Beispiel per App oder SMS auf das Handy geschickt wird. So erfüllt das Smartphone die Funktion der Bankkarte. Kriminelle können mit dem Passwort alleine nichts mehr anfangen, sie müssten zusätzlich an das Handy des Betroffenen kommen, um sich in den Account einzuloggen.

Mythos 4: Am besten merkt man sich Passwörter mit Stift und Papier

Jedes Konto sollte mit einem eigenen Passwort geschützt werden. Denn können Kriminelle ein Passwort knacken, haben sie nur Zugriff auf den einen Account und nicht auf andere Konten des Nutzers. Aber Internetnutzer haben oft Dutzende Accounts: Bank, E-Mail, Schnäppchen-Website und so weiter. Wie kann man sich die einzelnen Passwörter merken? Sie auf ein Post-it zu schreiben und an den Monitor zu heften: keine gute Idee. Neugierige Familienmit-glieder oder Arbeitskollegen können so ganz einfach auf sensible Daten zu-greifen, und es wird schnell unüber-sichtlich. Besser: einen Passwortmanager verwenden. So lassen sich auch Dutzende Konten recht einfach verwalten. So lässt sich mit geringem Aufwand eine Passwortdatenbank aufbauen. Der Nutzer muss sich nicht mehr zig Codes merken, sondern nur noch einen, nämlich das für den Passwortmanager. Dieses Masterpasswort sollte selbstverständlich klug gewählt werden und möglichst lang und komplex sein.

Mythos 5: Biometrische Passwörter sind sicherer als Textpasswörter

Warum sollte man sich komplizierte Passwörter merken, wenn man doch einzigartige Merkmale mit sich herumträgt? Schon jetzt lassen sich Smartphones per Fingerabdruck entsperren, mit der Iris, oder gleich dem ganzen Gesicht. Allerdings ist die Stärke von biometrischen Passwörtern gleichzeitig ihre Schwäche: die Einzigartigkeit. Wenn ein Passwort gestohlen wird, können Nutzer es einfach ändern. Aber wie soll man einen Fingerabdruck oder ein Gesicht ändern, wenn Kriminelle dieses Merkmal erbeutet haben? Gerade Fingerabdrücke lassen sich einfach kopieren. Wenn auf Fotos die Finger von vorne zu sehen sind, lassen sie sich nachmachen.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity