Passwort: Sesam öffne dich

Die Problematik beim Datenschutz ist, dass ein potenzieller Angreifer nur eine Lücke finden muss. Im Gegensatz dazu hat der Besitzer oder Nutzer von Systemen sehr viele Angriffspunkte und Schwachstellen zu verteidigen. Das bedeutet, dass jeder Zugang, jede Software, praktisch jedes Objekt geschützt werden müssen. Nachlässigkeit wird bestraft, denn wir wissen nicht, wann ein „Angriff" passieren wird. Experten meinen: „Es ist nur eine Frage der Zeit, bis man selbst betroffen ist."

Passwörter sind wie Schlüssel zu sehen, die man niemals verlieren und nicht weitergeben sollte. Sie sind neben den User- oder Zugangsdaten das wichtigste Schutzelement, um auf Systeme, Cloud oder Benutzerkonten zugreifen zu können. Sie sind ebenso bei der Verschlüsselung von Datenträgern und Sperren von Geräten bei Arbeitsunterbrechungen von essenzieller Bedeutung.

Stärke der Passwörter

Wichtig ist, ein „starkes" (d. h. ausreichend langes und nicht leicht zu knackendes) Passwort zu verwenden. Da Passwörter meist von Systemen (Software mit entsprechenden Programmen) gehackt werden und nicht von Menschen, sollte der maximale Schutz durch Kreativität erreicht werden. Sehr hilfreich ist es, ein Passwort aus einer langen, selbst erfundenen Passphrase zu erstellen. Es ist sinnvoll, dass diese aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen besteht. Sie sollte in keinem Wörterbuch aufscheinen oder ähnlich den allseits bekannten Passwörtern sein. Entscheidend, wie schnell ein Passwort entschlüsselt werden kann, sind die Länge (mindestens acht bis zwölf Zeichen) und eine Kombination von Groß- und Kleinbuchstaben, Zahlen oder Sonderzeichen. Länge schlägt Komplexität!

Auf keinen Fall sollte man Name, Vorname (den eigenen, des Partners, des Haustiers etc.) verwenden. Die Empfehlung lautet, für verschiedene Systeme verschiedene Passwörter zu vergeben. Auf jeden Fall muss eine Trennung der Privat- und Firmen-Passwörter erfolgen. Es darf keine Ähnlichkeiten geben, damit kein Rückschluss möglich ist, falls durch ein Leck ein Passwort korrumpiert wird. Wenn möglich keine Folge von Passwörtern (Zahlenfolge etc.) verwenden, um Rückschlüsse oder Interpolation zu verhindern.

Änderungshäufigkeit

Lange Zeit war die Änderungshäufigkeit kein Diskussionsthema. Es wurden firmeninterne Regelungen in einer Security Policy fixiert, wie ein Passwort gestaltet und in welchem Rhythmus es geändert werden muss. So weit sollten wir es auch in den technisch-/organisatorischen Maßnahmen der DSGVO dokumentiert haben.

> ***Man muss keinesfalls Experte sein, um seine digitalen Assets zu schützen.***

Interessant ist, dass in Deutschland aktuell eine Diskussion über die Änderungshäufigkeit stattfindet. Ausgelöst wurde diese durch eine Veröffentlichung des „Bundesamtes für Sicherheit in der Informationstechnik", siehe Link-Tipps. Meine Empfehlung dazu lautet: auf jeden Fall Passwörter ändern. Die Änderungshäufigkeit und den Rhythmus bestimmen Sie aufgrund Ihrer Erfahrung. Bitte aber nicht vergessen, dies im Verfahrensverzeichnis/TOM der DSGVO zu dokumentieren.

Aufbewahrung der Passwörter

Passwörter sind vor dem Zugriff von unberechtigten Personen zu schützen und sicher aufzubewahren. So weit die Theorie, aber bei ordnungsgemäßer Anwendung fallen dutzende Passwörter an, vielleicht auch über 100. Diese im Kopf zu behalten, ist sicher lobenswert, wäre aber eher ein Fall für „Wetten dass..?". Zur Dokumentation sollte man sich Hilfsmittel bedienen. Die verwerflichsten Varianten sind die gelben Zettel am Bildschirm, unter der Tastatur usw. Wenn schriftliche Aufzeichnungen, dann sollten sie in einem Tresor verwahrt werden. Besser wäre da schon eine Datei, die verschlüsselt sein muss. Die beste Lösung ist sicher eine entsprechende Software (App). Deren beide Schwachpunkte sind das sogenannte „Masterpasswort" einerseits und die Datenhaltung in der Cloud andererseits. (Siehe auch Link-Tipp: Heise-Passwortmanager.)

Tipps zu mobilen Geräten

Notebook, Smartphone oder Tablet-PC sollten durch ein Passwort, eine Geheimzahl oder durch ein biometrisches Merkmal (Fingerabdruck, Gesichtsscan) geschützt werden. Damit ist sichergestellt, dass es durch andere Personen nicht in Betrieb genommen werden kann (z. B. nach einem Diebstahl, im Kaffeehaus vergessen …). Somit bleiben Ihre Daten bei Verlust oder Diebstahl geschützt und das Gerät kann bei entsprechender Einrichtung aus der Ferne deaktiviert oder Daten können gelöscht werden. Man muss keinesfalls Experte sein, um seine digitalen Assets zu schützen. Einfach nur seine Hausaufgaben zu machen, bringt ein großes Stück Sicherheit. Und wie immer an dieser Stelle: den Hausverstand anwenden! Sollte die Materie zu komplex erscheinen, wenden Sie sich vertrauensvoll an Ihre Fachgruppe, die WKNÖ oder an einen IT-Experten Ihres Vertrauens.

Weitere Informationen:

Ein Online-Tool zur Überprüfung der Stärke eines Passworts.
Passwortmanager – Artikel von Heise.de
BSI verabschiedet sich vom präventiven regelmäßigen Passwort-Wechsel.
BSI - Identitäts- und Berechtigungsmanagement (Edition 2021)

Fotocredit: iStock.com/mattjeacock