IT-Sicherheitstipp Nr.4 – Juni 2019

Sichere Passwörter

Warum sollten Sie Passwörter verwenden?

Passwörter dienen der Zugangskontrolle. Sie sichern sensible und schützenswerte Daten, Systeme und Programme. Sie können ein Passwort mit Ihrem Haustürschlüssel vergleichen. Mit diesem kontrollieren Sie den Zugang zu Ihrem Haus. Genauso kontrolliert man mit dem Schlüssel "Passwort" den Zugang zu sensiblen Daten und Verfahren.

Wo werden Passwörter verwendet?

Passwörter werden bei Anmeldungen an Rechnern, Netzwerken, Netzlaufwerken und Computeranwendungen verwendet. Sie schützen Ressourcen wie Dateien und Informationen vor unberechtigtem Lesen, Schreiben, Ändern oder Löschen.
Auch der Zugang zu einzelnen Programmen wird häufig durch Passwörter geschützt. Zum Beispiel können nur Sie, mit Ihrem Anmeldenamen und Ihrem Passwort, Ihre E-Mails lesen.

Wie sieht ein sicheres Passwort aus?

Der Name Ihres Lebenspartners oder Ihrer Lebenspartnerin, Ihr Autokennzeichen, Ihr Geburtsdatum oder Ihre Telefonnummer stellen keine guten Passwörter dar. Sie könnten leicht erraten oder abgeleitet werden. Auch Fremdwörter oder Wörter einer anderen Sprache sind keine gute Wahl, da diese mit automatisierten Verfahren über sog. Wörterbuch- oder Brute-Force-Angriffe durch Erraten "geknackt" werden können.

Ein sicheres Passwort ist mindestens zwölf Zeichen lang und besteht aus einer Kombination von großen und kleinen Buchstaben, Ziffern und Sonderzeichen wie z.B. Ausrufezeichen oder Fragezeichen. Außerdem sollten keine Buchstaben genutzt werden, die auf der Tastatur direkt nebeneinander liegen. Idealerweise sollte das Passwort einmalig sein.

****

Passwörter merken

„Merksatz-Methode“

Sie könnten ein Sprichwort, eine Liedzeile oder einen Begriff in Kombination mit Ziffern und Sonderzeichen verwenden, um daraus ein Passwort zu erstellen. Aus einer Frage "Sind Siebenmeilenstiefel schnell?" wird durch die Ersetzung des Wortes Sieben durch die Zahl "7", Meilen durch die Abkürzung "km" und die Ersetzung des Buchstabens "i" durch ein Ausrufezeichen das Passwort: Sind7kmSt!efelSchnell?

Ein Trick, um mehrere sichere Passwörter für verschiedene Anwendungen oder Internetseiten zu haben: Bilden Sie wie hier geschildert ein Passwort und stellen Sie diesem bei jeder Anwendung oder Internetseite ein individuelles Kürzel voran (Amazon = Ama).

Cybersicherheit

Oftmals haben Sie aber nicht nur eins, sondern sogar mehrere Passwörter zu verschiedenen Systemen. Das ist gut für die Sicherheit, denn sollte eines Ihrer Passwörter einem Dritten bekannt geworden sein, kann er nicht weitere Zugänge auch noch übernehmen.
Mit einer zunehmenden Zahl von komplexen Passwörtern wird es allerdings auch immer schwieriger sich diese zu merken. Helfen kann Ihnen da ein sogenannter **"Passwortmanager".**

Beispiele für sichere Passwörter:

- Sind7kmSt!efelSchnell?
- 1Z0ll=2,54cm (1 Zoll entspricht 2,54 Zentimeter)
- 0221idVv#K (0221 ist die Vorwahl von #Köln)
- WdP15mkuiz6MadBgb! (Wenn der Postbote 15 mal klingelt und ich zum 6 Mal aus dem Bett gefallen bin)
- Grundpasswort: Ich habe fünf Finger an jeder meiner Hände = Ih5F@jmH
- Variante für PC-Anmeldung: PCIh5F@jmH
- Variante für E-Mail-Programm: EMIh5F@jmH
- Variante für Melderegisterverfahren: MRIh5F@jmH

KeePass

Das ist ein Hilfsprogramm, welches sich Ihre Passwörter merkt und sicher auf dem Computer aufbewahrt. Zugang dazu haben Sie über ein besonders sicheres Passwort, das Masterpasswort. In Zukunft müssen Sie sich also nur noch ein Passwort merken, alle weiteren stecken dahinter. Ein Beispiel für einen Passwortmanager ist das Programm „KeePass“. KeePass ist kostenlos und frei verfügbar.

Durch Open Source (offener Quellcode) kann jeder nachvollziehen, dass dieses Programm sicher mit Ihren Passwörtern umgeht. KeePass können Sie direkt auf der Herstellerwebseite herunterladen: https://keepass.info
Außer diesem Manager gibt es noch viele weitere Lösungen und Produkte um Ihre Passwörter zu verwalten. Auch im privaten Bereich ist der Einsatz eines Passwortmanagers empfehlenswert.

Achtung: Bitte besprechen Sie einen Download und die dienstliche Nutzung vorher mit Ihren IT-Ansprechpartnern (siehe Kontakt).

Richtiger Umgang mit Passwörtern

Wenn Ihr Passwort auf einem Zettel am Monitor klebt, können alle, die in Ihr Büro kommen, dieses lesen (übrigens zählen auch die Zettel unter der Tastatur dazu).
Würden Sie die PIN Ihrer Bank-Karte öffentlich an die Tafel schreiben oder Ihren Haustürschlüssel zum Nachmachen auslegen?!

Aus dem gleichen Grund gilt:

- Passwörter dürfen nirgends notiert werden!
- Achten Sie bei der Eingabe darauf, dass Sie niemand beobachtet. Es ist nicht unhöflich, Anwesende darum zu bitten wegzusehen!

Weitergabe von Passwörtern

Passwörter dürfen nicht weitergegeben werden!

Das Aushorchen von Passwörtern ist eine beliebte Methode, um an vertrauliche Daten zu gelangen. Hier sollten Sie sehr vorsichtig sein! Ein Passwort ist geheim und personengebunden. Alle berechtigten Personen können über die zuständige Organisationseinheit ein eigenes Passwort erhalten. Sie benötigen nicht das Ihrige.
Auch Kriminelle wollen Ihr Passwort z.B. telefonisch, unter Vorspiegelung falscher Tatsachen, erfragen.
Auch das "Eben-mal-Aushelfen" für eine Kollegin oder einen Kollegen ist kritisch, wenn Sie dafür Ihr Passwort weitergeben. Oft werden Zugriffe auf passwortgeschützte Systeme protokolliert. Wenn Ihr Kollege oder Ihre Kollegin einen Fehler mit Ihrem Passwort macht, wird man zuerst auf Sie zukommen.

Cybersicherheit

So verhalten Sie sich richtig, falls Sie nach Ihrem Passwort gefragt werden:

- Geben Sie Ihr Passwort niemals weiter, auch nicht an Kolleginnen oder Kollegen
- Fragen Sie den Anrufer/die Anruferin nach Name, Dienststelle und Telefonnummer
- Rufen Sie zurück, nach dem Sie sich über das Anliegen anderweitig versichert haben
- Melden Sie einen Vorfall Ihren Vorgesetzten, ggf. Ihren IT-Ansprechpersonen (siehe Kontakt)

Ausspionieren von Passwörtern

Gefahren lauern schon bei der Passwort-Eingabe!

Wer kann auf Ihrer Tastatur mitlesen, wenn Sie Ihr Passwort eingeben, z.B. durch die Bürotür oder ein Bürofenster? Achten Sie darauf, dass Sie möglichst niemand bei der Eingabe des Passwortes beobachten kann.

Bislang müssen Passwörter aufgrund technischer oder organisatorischer Vorgaben wiederkehrend geändert werden. Mittlerweile wird vermehrt empfohlen, möglichst lange Passwörter zu verwenden, die dafür in größeren zeitlichen Abständen geändert werden müssen. Wenn Sie befürchten, dass jemand Ihr Passwort erraten hat, ändern Sie es sofort!

Übrigens:

Nicht nur Menschen können spionieren, sondern auch Computerprogramme, z.B. Viren. Manche dieser Computerviren sind in der Lage, Ihre Passworteingabe aufzuzeichnen und per E-Mail zu versenden.