Sicherheit von Passwörtern und Zugangsdaten

KeePass (Passwort-Verwaltungsprogramm)

Für E-Mail-Konten, Online-Shops, Online-Speicher, Online-Banking, Reisebuchungen, Mitgliederbereiche von Vereinen, eigene Internetseiten, Foren, soziale Netzwerke u.v.m. muss man sich im Internet mit einem Benutzernamen beziehungsweise mit der E-Mail-Adresse und einem Passwort anmelden.

Solche Zugangsdaten interessieren auch kriminelle Hacker, wie die kürzlich entdeckten Datendiebstähle von vielen Millionen digitalen Identitäten zeigen.

→ Datendiebstahl im großen Rahmen
z. B. Hacken von Datenbanken von Unternehmen, Providern pp.)
aber auch Nutzung, Weitergabe oder Verkauf der Daten durch „schwarze Schafe" unter den Berechtigten.

→ Hacken von Zugangsdaten einzelner Accounts / Benutzerkonten.

Mit den Zugangsdaten können Kriminelle frei über das Benutzerkonto verfügen. Je nach Art können sie z. B. die Lieferadresse ändern und Waren bestellen, das Profil ändern, falsche Nachrichten posten, Privates einsehen oder Mails mitlesen und sogar über diesen Account Mails schreiben.

Sie können auch die Zugangsdaten ändern, so dass der rechtmäßige Besitzer nicht mehr auf sein eigenes Konto zugreifen kann.

Video 01 (nicht mehr verfügbar)

Zum Video:

Hacker >>> Brute-Force-Angriffe (vollautomatisches Knacken von Passwörtern mit Hilfe von einer Vielzahl von Zeichenkombinationen auf Grundlage von Wörterbüchern u.v.m)

Rasante Entwicklung > Verhältnis Rechnergeschwindigkeit - Passwortlänge

Passwörter

→ Grundsätzlich sollte man für jeden Account / für jedes Benutzerkonto ein eigenes Passwort vergeben. Das begrenzt den Schaden, falls doch einmal ein Account / Benutzerkonto gehackt werden sollte.

→ Passwörter regelmäßig ändern.

→ Länge des Passwortes je nach Sicherheitsbedürfnis.

→ Ein gutes Passwort sollte mindestens zwölf Zeichen lang sein.
(Ausnahme: Bei Verschlüsselungsverfahren wie zum Beispiel WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren - das geht beim Hacken von Online-Accounts in der Regel nicht.)

→ Tabu sind alle Wörter, die einen Sinn ergeben, Namen von Familienmitgliedern, des Haustieres, des besten Freundes, Kosenamen, Geburtsdaten, Autokennzeichen, aber auch typische Muster auf der Tastatur wie „qwertz".
Es sollte auch nicht in Wörterbüchern vorkommen.

→ Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen, ist auch nicht empfehlenswert.

→ Wichtiger als die Länge des Passwortes ist der Mix aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

→ Problem Umlaute, aber auch Sonderzeichen, welche man sich über die Ziffern der jeweiligen Taste auf der Tastatur merkt.

→ Problem Funktion „Passwort vergessen"
Nachdem man das neue Passwort per E-Mail erhalten hat, das Passwort sofort ändern! *(E-Mail-Verkehr ist immer unsicher!)*

→ Problem „Ersatzfragen" bei Verlust des Passwortes
(Name der ersten Schule, Beruf des Großvaters, Geburtsname der Mutter, mein Lieblingsverein, mein erstes Auto .....)

Eselsbrücken bauen

Da gibt es viele Möglichkeiten, aber auf Dauer kann man sich nur wenige merken.

IwiNubd3.KmE

Ich **w**ohne **i**n **N**ettetal **u**nd **b**in **d**as **3. K**ind **m**einer **E**ltern

Passwörter mit System

Für jeden Account bleibt das „Basispasswort“ gleich. Allerdings werden für jeden Account individuell Zeichen eingeschoben.

IwiN###ubd3.KmE

Beispiel: „IwiN**Ama**ubd3.KmE“ für das Kundenkonto bei **Ama**zon.

Passwort-Verwaltungsprogramm (Passwortmanager)

Wem das alles zu viel ist, der nutzt einen sogenannten Passwort-Manager. Das ist ein kleines Computerprogramm, das Passwörter generiert und verschlüsselt speichert. Man muss sich nur noch ein einziges Passwort, ein sogenanntes Master-Passwort merken.

Siehe auch Tipps vom BSI: *(Ausschnitt)*

Passwörter notieren?

Bundesamt für Sicherheit in der Informationstechnik

Passwörter sollten niemals unverschlüsselt auf dem PC abgelegt werden oder auf dem berühmten Notizzettel am Bildschirm kleben. Wer sich Passwörter notieren will, sollte diese stattdessen auf Papier unter Verschluss halten bzw. auf dem Rechner in einer verschlüsselten Datei ablegen. Wer viele Online-Accounts hat, für den empfiehlt sich ein **Passwort-Verwaltungsprogramm** wie zum Beispiel keepass.
Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter generieren (berücksichtigen Sie jedoch bei den Einstellmöglichkeiten zur Passwortgenerierung unsere oben genannten Mindestempfehlungen). Sie müssen sich dann nur noch **ein gutes Masterpasswort** überlegen und merken.

Video 02 (PC WELT - Infos und Video über KeePass)

http://www.pcwelt.de/downloads/Passwortschutz-KeePass-569451.html

Download von der Herstellerseite

Programm: http://keepass.info/download.html

Übersetzung: http://keepass.info/translations.html

KeePass → Classic Edition

KeePass2 → Professional Edition

Die Datenbankdateien der beiden Versionen sind nicht kompatibel.
Allerdings ist das Im- bzw. Exportieren der Datensätze gegenseitig möglich.

Möglichkeit der Nutzung auf Smartphone und Tablet

Für Android → KeePassDroid (kostenlos)

Für iPad / iPhone → MyKeePass (0,89 €)

Die App installieren und die Datei mit der verschlüsselten Datenbank (*.kdb) hinzufügen.