Passwörter

Wer die Wahl hat, hat die Qual – heißt es. Besonders bei der **Wahl der richtigen Passwörter** tun sich viele PC-Nutzer schwer. Um dem zu entgehen, kommt es nicht selten vor, dass jemand ein Passwort für zehn verschiedene Programme beziehungsweise Zugänge hat. Wen wundert's da, dass schlecht gewählte Passwörter auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen. Hacker freut das natürlich. Sie haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Deshalb: Orientieren Sie sich an den folgenden Empfehlungen – und schon tun Sie etwas mehr für Ihre Sicherheit.

Tipps

Ein gutes Passwort

- Es 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 zum Beispiel beim Hacken von Online-Accounts nicht.)
- Es sollte aus **Groß- und Kleinbuchstaben** sowie **Sonderzeichen und Ziffern (?!%+…)** bestehen.
- Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter.
- Wenn möglich sollte es **nicht in Wörterbüchern** vorkommen.
- Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, **also nicht asdfgh** oder **1234abcd** und so weiter.
- 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.

Bitte beachten Sie: Wenn Ihr System Umlaute zuläßt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese evtl. nicht eingegeben werden können.

Passwörter notieren?

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 (Eine deutsche Sprachdatei für dieses englischsprachige Programm gibt es auf der Herstellerseite). Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter

generieren (berücksichtigen Sie bei den Einstellmöglichkeiten zur Passwortgenerierung unsere oben genannten Mindestempfehlungen). Sie müssen sich dann nur noch **ein gutes Masterpasswort** überlegen und merken.

Wie merkt man sich ein gutes Passwort?

Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. **Hier ein Beispiel:**
"**M**orgens **s**tehe **i**ch **a**uf **u**nd **p**utze **m**ir **m**eine **Z**ähne **d**rei **M**inuten **l**ang." Nur die ersten Buchstaben: "**MsiaupmmZdMl**". "i und l" sieht aus wie "1", "&" ersetzt das "und": "**Ms1a&pmmZ3M1**".
Auf diese Weise hat man sich eine gute "Eselsbrücke" gebaut. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren.

Wichtig ist hierbei, dass sich der Benutzer des Passwortes den Satz **selbst ausgedacht** hat. Werden zum Beispiel die Anfangsbuchstaben eines Literaturzitates als Passwort gewählt, dann ist prinzipiell die **Möglichkeit einer Wörterbuchattacke** nicht viel unrealistischer, als wenn direkt ein Wort verwendet würde. Dies trifft natürlich insbesondere für weithin bekannte Zitate zu.
Grundsätzlich sinnvoll ist es immer, echten Zufall in den Prozess der Auswahl eines Passwortes zu integrieren. Zum Beispiel kann man durch den Wurf einer Münze entscheiden, ob ein "und" im zugrundeliegenden Satz durch ein u oder durch & dargestellt wird.

Passwörter regelmäßig ändern

Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern Sie automatisch daran, wenn Sie das Passwort zum Beispiel schon ein halbes Jahr benutzen. Diese Aufforderung nicht gleich wegklicken – sondern ihr am besten gleich nachkommen! Natürlich ist es da schwer, sich alle Passwörter zu merken. Womit wir beim nächsten Punkt sind.

Keine einheitlichen Passwörter verwenden

Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke beziehungsweise Zugänge (Accounts) zu verwenden, also ein und dasselbe Passwort für das Online-Banking und für Soziale Netzwerke zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, hat der Angreifer freie Bahn für Ihre übrigen Anwendungen. Das können zum Beispiel die Mailbox oder alle Informationen auf dem PC sein.

Voreingestellte Passwörter ändern

Bei vielen Softwareprodukten werden bei der Installation (beziehungsweise im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Hacker wissen das: Bei einem Angriff probieren sie zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Deshalb ist es ratsam, in den Handbüchern nachzulesen, ob solche Accounts vorhanden sind und wenn ja, diese unbedingt mit individuellen Passwörtern abzusichern.

Bildschirmschoner mit Kennwort sichern

Bei den gängigen Betriebssystemen haben Sie die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit zu sperren. Die Entsperrung erfolgt erst nach Eingabe eines korrekten Passwortes. Diese Möglichkeit sollten Sie nutzen. Ohne Passwortsicherung können unbefugte Dritte sonst bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen. Natürlich ist es ziemlich störend, wenn die Sperre schon nach weniger Zeit erfolgt. Unsere

Empfehlung: 5 Minuten nach der letzten Benutzereingabe. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren (zum Beispiel bei einigen Windows-Betriebssystemen: Strg+Alt+Entf drücken).

Passwörter nicht an Dritte weitergeben oder per E-Mail versenden

In der Regel werden E-Mails unverschlüsselt versandt. Unverschlüsselte E-Mails können von Dritten auf ihrem Weg durch das Internet mitgelesen werden. Zudem können E-Mails im Internet verloren gehen oder herausgefiltert werden. Der Absender einer E-Mail hat daher keine Gewissheit, dass seine Nachricht den gewünschten Empfänger auch wirklich erreicht hat. Wenn Sie ihre Passwörter an Dritte weitergeben, verlieren Sie die Kontrolle darüber und Sie haben sich umsonst die Mühe für ein gutes Passwort gemacht.

Recherchiert am 05.11.2014; gefunden unter: https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html