Tipps zum Umgang mit Passwörtern

05.10.2024 03:21:49

FAQ-Artikel-Ausdruck

Kategorie:	Anwenderbetreuung::Allgemein	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	12:46:23 - 01.10.2020

Schlüsselwörter

Benutzerkennung; Passwort; Sicherheit

Symptom (öffentlich)

Welche Tipps können Sie mir zum Umgang mit Passwörtern geben?

Problem (öffentlich)

Lösung (öffentlich)

Tipps zum Umgang mit Passwörtern

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 sie stattdessen gut 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. 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: "Morgens stehe ich auf und putze mir meine Zähne drei Minuten lang." 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, etwa das Aneinanderreihen von beliebigen, zusammenhanglosen Wörtern. Ein Beispiel - was Sie dann natürlich nicht selbst verwenden sollten: "Ein blaues Pferd liest Kaffeesatz auf dem Ausflugsdampfer".
Außerdem ist es ratsam, dass sich der Benutzer des Passwortes den Satz selbst ausgedacht hat. Wird als Merksatz zum Beispiel ein bekanntes Literaturzitat oder eine Liedzeile als Passwort gewählt, so ist es wahrscheinlich, dass Angreifer auch dies mittels einer Wörterbuchattacke herausfinden können.

Änderung von Passwörtern
Zunächst sollten Sie sich Gedanken machen, welche Ihrer Passwörter besonders viele oder sensible persönliche Daten schützen. Ein wichtiges Passwort ist zum Beispiel Ihr Passwort für Ihr privates E-Mail-Konto. Dort sind nicht nur persönliche Nachrichten und Kontakte hinterlegt, sondern mithilfe des Zugangs zu Ihrem E-Mail-Account lassen sich auch viele andere Passwörter in von Ihnen genutzten Online-Diensten zurücksetzen und neu vergeben. Andere Beispiele für wichtige Passwörter sind die Passwörter für Profile in sozialen Netzwerken, für den Zugang zu häufig genutzten Online-Shops oder andere regelmäßig genutzte elektronische Identitäten. Diese wichtigen Passwörter sollten in regelmäßigen Zeitabständen geändert werden, mindestens einmal jährlich. Eine solche eigenständige Änderung ohne externen Anlass macht Ihre Zugangsdaten für Dritte wertlos, sollten sie ohne Ihr Wissen entwendet worden sein. Einige Programme und Dienstleister erinnern Sie automatisch daran, wenn Sie das Passwort schon längere Zeit benutzen.
Ein Passwort sollte auf jeden Fall geändert werden, wenn es einen Hinweis gibt, dass es tatsächlich in die Hände von unbefugten Dritten gelangt ist. Ein solcher Hinweis kann beispielsweise die direkte Aufforderung eines Diensteanbieters sein, das Passwort zu ändern, ebenso die Nachricht, dass Passwörter eines bestimmten Dienstleisters gestohlen worden und nun im Internet aufgetaucht sind. Auch eine Spam- oder Phishing-Mail, in der korrekte persönliche Daten genutzt werden, kann ein Hinweis darauf sein, dass jemand Zugang zu einem privaten Account hatte und dort Daten abgriff.
Sollten Sie feststellen, dass Ihr Gerät mit einem Schadprogramm infiziert ist, ist dies ebenfalls ein Grund, Passwörter zu ändern. Manche Varianten von Schadprogrammen zeichnen Zugangsdaten auf und übermitteln diese an Dritte. Um dies zu unterbinden, muss zunächst das Gerät bereinigt werden. Erst anschließend sollten die Passwörter geändert und Log-Ins wieder über das betroffene Gerät durchgeführt werden.
Zugangsdaten, die Cyber-Kriminelle bei Anbietern oder direkt bei Nutzerinnen und Nutzern abgegriffen haben, werden anschließend oft im Internet veröffentlicht oder zum Kauf angeboten. Diese Datensätze kursieren dann im Netz. Je länger darin enthaltene Zugangsdaten nicht geändert werden, desto mehr Dritte können sie für ihre Zwecke nutzen. Im Internet gibt es unterschiedliche Portale, über die überprüft werden kann, ob persönliche Zugangsdaten in einem solchen bekanntgewordenen Datensatz enthalten sind. Ein deutschsprachiges Angebot ist beispielsweise der HPI Identity Leak Checker,

ein internationaler Anbieter haveibeenpwned.com. Das BSI kann keine Aussage zu der Qualität und Aktualität der dort hinterlegten Daten treffen. Grundsätzlich ist bei der Nutzung solcher Portale zu beachten, dass für Zugangsdaten häufig die Kombination aus E-Mail-Adresse und Passwort verwendet wird. In den Datenbanken wird allerdings in der Regel nur die E-Mail-Adresse mit dem Datenbestand abgeglichen. Die Rückmeldung, dass die E-Mail-Adresse in dem Datenbestand enthalten ist, kann sich also auf jeden Account beziehen, bei dem diese E-Mail-Adresse zum Zugang genutzt wird, eine direkte Zuordnung ist nicht möglich.

Keine einheitlichen Passwörter verwenden
Viele Anwender denken sich ein Passwort aus und nutzen dieses dann für mehrere Online-Accounts, damit sie sich nicht viele verschiedene Passwörter merken müssen. Dieser Ansatz ist bequem, aber dennoch nicht zu empfehlen, selbst wenn das gewählte Passwort den oben genannten Kriterien entspricht. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, hat der Angreifer freie Bahn für alle weiteren Accounts mit dem gleichen Passwort. Er kann einfach automatisiert durchtesten, wo dieses Passwort ebenfalls verwendet wird.

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, die voreingestellten Passwörter zu ändern.

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 störend, wenn die Sperre schon nach kurzer Zeit erfolgt. Unsere Empfehlung: Fünf Minuten nach der letzten Benutzereingabe sollte der Bildschirmschoner anspringen und damit die Sperrung erfolgen. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren. Bei einigen Windows-Betriebssystemen erfolgt dies beispielsweise durch die Tastenkombination Strg+Alt+Entf.

Passwörter nicht an Dritte weitergeben oder per E-Mail versenden
In der Regel werden E-Mails unverschlüsselt versandt und können so 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. Aus diesen Gründen sollten Sie Passwörter nicht per E-Mail versenden.
Grundsätzlich gilt zudem: Wenn Sie Ihre Passwörter an Dritte weitergeben, verlieren Sie damit in gewisser Weise die Kontrolle, weil diese Dritten nun theoretisch die entsprechenden Dienste nutzen und die dort hinterlegten Informationen ändern können. So haben Sie sich umsonst die Mühe für ein gutes Passwort gemacht.

Quellen und weiterführende Informationen
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html