

WURDE IHR PASSWORT AUCH SCHON IM INTERNET VERÖFFENTLICHT? DER WEG ZUM SICHEREN PASSWORT

Regelmäßig gelangen Hacker und Online-Kriminelle an Zugangsdaten. Nicht selten gelangen diese Angreifer dann an mehrere Tausend bis Millionen Datensätze. Immer wieder werden diese Datensammlungen dann auch veröffentlicht. Das Hasso-Plattner-Institut sammelt diese Datensätze und hatte Anfang Dezember 2019 rund 10 Milliarden Zugangsdaten im Bestand.

Nutzen Sie ein Top-100-Passwort?

Das Hasso-Plattner-Institut hat die gesamten Zugangsdaten ausgewertet und eine Statistik der am häufigsten verwendeten Passwörter erstellt. Interessanterweise werden auch heute oft noch sehr einfache Passwörter verwendet, wie „123456“, „123456789“ und „password“.

Anforderungen an ein Passwort

Das große Problem bei kurzen und einfachen Passwörtern ist, dass diese häufig auch einfach geknackt, also erraten oder z. B. über Tabellen ermittelt werden können.

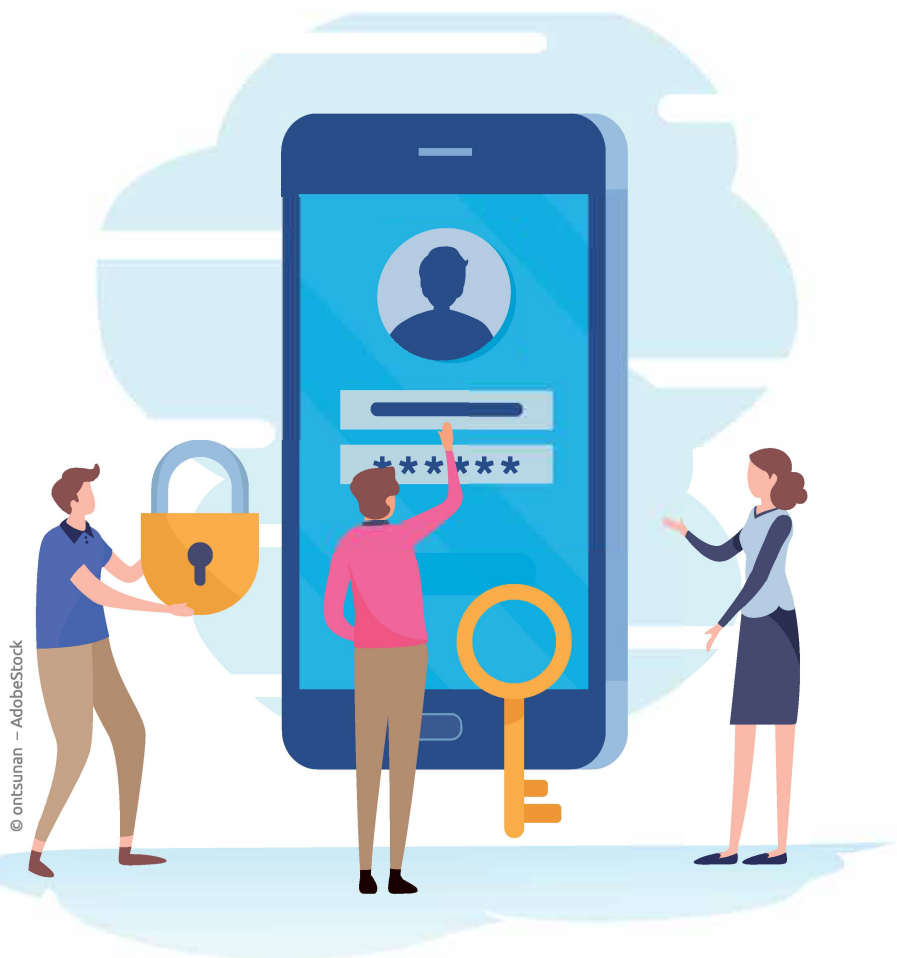
Um es Angreifern schwerer zu machen, sollte das Passwort nicht im Wörterbuch stehen und keine Wiederholungs- oder Tastaturmuster enthalten, wie beispielsweise „123...“ oder „qwertz“. Damit neugierige Kollegen oder Familienmitglieder nicht heimlich an Ihre Daten gelangen, sollten auch keine persönlichen Angaben wie Geburts- oder Hochzeitsdatum, Namen oder Hobbys verwendet werden. Aus diesen Gründen sollten die Passwörter aus einer Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

Zudem sollten Passwörter möglichst lang sein und wenn möglich zehn Zeichen und mehr umfassen. Kürzere Passwörter sollten möglichst nur zum Einsatz kommen, wenn zusätzliche Sicherheitsmaßnahmen vorhanden sind und z. B. nach drei Fehlein-

gaben der Zugang gesperrt wird. Zu guter Letzt sollten die Passwörter auch nicht durch Dritte einsehbar sein. Die Passwörter sollten somit nicht auf bzw. unter Schreibunterlagen oder auf Notizzetteln am Monitor zu finden sein.

Einfach ein Passwort wie „lss10JF&hetT“ merken?!

Sofern Sie kein Programm zur Passwortverwaltung nutzen dürfen oder möchten, können Sie sich einfach mit einem Passwortsatz kryptische Passwörter erstellen und merken. Dazu suchen Sie sich einen Satz aus, der möglichst viele Wörter, mindestens eine Zahl und möglichst ein Sonderzeichen enthält, z. B. „Ich spiele seit 10 Jahren Fußball & habe ein tolles Team“. Jeweils das erste Zeichen sowie die Zahl und das Sonderzeichen ergeben dann das Passwort. ➤



> Jeder Log-in benötigt ein individuelles Passwort

Viele Menschen verwenden für unterschiedliche Anwendungen, Webseiten, Dienste und Apps dieselben Zugangsdaten. Online-Kriminelle nutzen dies immer wieder aus und versuchen, mit den erbeuteten Zugangsdaten Zugriff auf häufig genutzte Online-Shops und Dienste zu erhalten.

Da sich leider Sicherheitslücken nicht ausschließen lassen, sollten Sie für jeden Log-in auch ein eigenes Passwort benutzen. Sofern kein Passwortmanager zur Verwaltung der Zugangsdaten zur Verfügung steht, können Sie dies z. B. dadurch erreichen, dass Sie das vorhandene Passwort um Buchstaben der jeweiligen Anwendung erweitern. Möglichkeiten wären z. B. der zweite und erste Buchstabe oder der letzte und der erste Buchstabe. Aus dem Passwort „Iss10JF&hetT“ für Windows dann beispielsweise „Iss10JF&hetTsW“.

Zugriff zusätzlich mit 2. Faktor absichern

Insbesondere die Betreiber von Online-Anwendungen, Marktplätzen und sozialen Netzwerken bieten immer häufiger eine Zwei-Faktor-Authentifizierung an. Neben einem Benutzernamen und Kennwort ist meistens dann die Eingabe eines zweiten Faktors, häufig eines Zahlencodes, erforderlich. Je nach Anbieter kann dies eine SMS an die hinterlegte Mobilfunknummer oder ein Zahlencode sein, den eine App auf dem Smartphone anzeigt.

Die Einrichtung ist meistens sehr einfach und schnell umzusetzen. Gelangt ein Krimineller an Ihre Zugangsdaten, bleibt er dank des zweiten Faktors außen vor, denn das Gerät, welches den Zahlencode per SMS erhält bzw. mit der installierten App generiert, ist nur in Ihren Händen.

Am 1.2.2020 ist nationaler „Ändere-dein-Passwort-Tag“

Auch wer ein sicheres Passwort hat, sollte es immer wieder ändern, sofern der Zugang nicht zusätzlich durch einen zweiten

Faktor gesichert ist. Denn es kann leider nicht ausgeschlossen werden, dass durch Schadsoftware, Fehler oder einen Trick das Passwort unbemerkt in falsche Hände gelangt.

Je mehr Schaden durch einen fremden Zugriff entstehen kann und je sensibler die Daten sind, die in der Anwendung verwaltet werden, desto häufiger sollte auch das Passwort geändert werden.

Am 1.2.2010 ist wieder der nationale „Ändere-dein-Passwort-Tag“. Einige Medien informieren an diesem Tag über die Wichtigkeit von sicheren Passwörtern und erinnern somit daran, jährlich das Passwort zu wechseln. Vorgegebene Passwörter von Geräten und Anwendungsprogrammen sollten Sie möglichst direkt bei der Inbetriebnahme ändern.

Sollten Sie den Verdacht haben oder darüber informiert werden, dass Unbefugte Ihr Passwort kennen, sollte natürlich direkt eine Änderung erfolgen.

Tipp

Sind meine Daten im Internet veröffentlicht?

Auf der Webseite <https://sec.hpi.de/ilc/> können Sie durch Eingabe Ihrer E-Mail-Adresse prüfen, ob auch Ihre Zugangsdaten in einer dieser Datensammlungen vorhanden sind. Das Ergebnis bekommen Sie per E-Mail gesendet.

Checkliste: Sicheres Passwort

Wenn möglich 10 Zeichen, besser mehr!	●
Groß- und Kleinbuchstaben	●
Zahlen und Sonderzeichen	●

Checkliste: Passworteinsatz

Separates Passwort je Anwendung bzw. Service	●
Vorgegebene Passwörter möglichst ändern	●
Regelmäßige Änderung der Passwörter	●
Sichere Verwahrung der Passwörter	●
Zusätzliche Sicherheitsmaßnahmen nutzen, z. B. zweiten Faktor	●
Standardpasswörter ändern	●