Der monatliche Security Awareness Newsletter für Jedermann

Einfache Passwörter erzeugen

Übersicht

Ihnen wird oft gesagt, dass Ihre Passwörter der Schlüssel zum Schutz Ihrer Konten sind (Das ist wahr!), aber selten erhalten Sie eine einfache Möglichkeit, alle Ihre Passwörter sicher zu erstellen und zu verwalten. Im Folgenden werden drei einfache Schritte beschrieben, um Ihre Passwörter zu vereinfachen, Ihre Konten abzusichern und Ihre Zukunft zu schützen.

Passphrasen

Die Zeiten verrückter, komplexer Passwörter sind vorbei. Diese Passwörter sind schwer zu merken, schwer zu tippen und mit den heutigen superschnellen Computern kann es für einen Cyber-Angreifer ein Leichtes sein, sie zu knacken. Die Länge der Passwörtern ist der Schlüssel zur Sicherheit, je mehr Zeichen Sie haben, desto besser. Eine Möglichkeit sind Passphrasen, eine Art starkes Passwort, das einen kurzen Satz oder zufällige Wörter verwendet. Hier sind zwei Beispiele

Zeit für starken Kaffee!
einsame-Schnecke-kriecht-Strand

Mit über zwanzig Zeichen sind beide stark. Außerdem sind sie leicht zu merken und einfach zu tippen, aber schwer zu knacken. Sie werden auf Websites oder Situationen stoßen, wo Sie Symbole, Zahlen oder Großbuchstaben zu Ihrem Passwort hinzufügen müssen, aber das ist in Ordnung. Aber behalten Sie im Hinterkopf, es kommt auf die Länge des Passworts an.

Passwort-Manager

Sie benötigen für jedes Konto ein eindeutiges Passwort. Wenn Sie das gleiche Passwort für mehrere Konten wiederverwenden, bringen Sie sich in große Gefahr. Ein Cyber-Angreifer muss nur eine Webseite, die Sie benutzen, hacken und alle Passwörter, einschließlich Ihrer, stehlen. Anschließend kann er sich mit Ihrem Passwort bei all Ihren anderen Konten anmelden. Es passiert viel öfter, als Sie denken. Sie glauben es nicht? Besuchen Sie die Webseite www.haveibeenpwned.com. Hier können Sie erfahren, ob Webseiten die Sie verwenden gehackt wurden und Ihre Passwörter möglicherweise gefährdet sind. Was sollten Sie also tun? Verwenden Sie einen Passwort-Manager.

Dies sind spezielle Computerprogramme, die alle Ihre Passwörter sicher in einem verschlüsselten Tresor speichern. Sie müssen sich nur ein Passwort merken, und zwar dasjenige für Ihren Passwort-Manager. Der Passwort-Manager ruft dann automatisch Ihre Passwörter ab, wenn Sie diese benötigen und meldet Sie auf den jeweiligen Webseiten an. Passwort-

Manager haben auch andere Funktionen, wie das Speichern Ihrer Antworten auf geheime Fragen, die Warnung, wenn Sie Passwörter wiederverwenden, einen Passwort-Generator, der sicherstellt, dass Sie sichere Passwörter verwenden, und viele andere Funktionen. Die meisten Passwort-Manager synchronisieren die Passwörter auch auf sicheren Weg auf fast jedem Computer oder Gerät, so dass Sie, unabhängig vom verwendeten System, einen einfachen und sicheren Zugriff auf alle Ihre Passwörter haben.

Sie sollten das Passwort für Ihren Passwort-Manager aufschreiben und an einem sicheren Ort in Ihrem zu Hause aufbewahren. Einige Passwort-Manager erlauben es Ihnen sogar, eine Anleitung für die Notfall-Wiederherstellung auszudrucken. Auf diese Weise haben Sie beim Verlust des Passworts für Ihren Passwort-Manager eine Art Absicherung. Auch wenn Sie krank werden oder sich in einem Notfall befinden, kann Ihr Ehepartner oder ein vertrauenswürdiges Familienmitglied so die Informationen in Ihrem Namen abrufen.

Zweistufige Verifizierung

Die zweistufige Verifizierung (oft als Zwei-Faktor-Authentifizierung oder Mehr-Faktor-Authentifizierung bezeichnet) bietet eine zusätzliche Sicherheitsebene. Diese erfordert, dass Sie zwei Dinge haben, wenn Sie sich bei Ihren Konten anmelden, Ihr Passwort und einen Zahlencode, der von Ihrem Smartphone generiert oder an Ihr Handy gesendet wird. Wenn ein Cyber-Angreifer Ihr Passwort in seinem Besitz hat, stellt dieser Prozess sicher, dass er trotzdem keinen Zugriff auf Ihre Konten erlangen kann. Die zweistufige Verifizierung ist einfach einzurichten. Sie muss in der Regel nur einmal verwendet werden, z.B. wenn Sie sich von einem neuen Computer oder Gerät aus anmelden. Aktivieren Sie die zweistufige Verifizierung wann immer möglich. Insbesondere für Ihre wichtigsten Konten, wie Ihre Bank- oder Pensionskonten oder für den Zugriff auf Ihre E-Mails. Wenn Sie einen Passwort-Manager verwenden, empfehlen wir Ihnen dringend, ihn mit einer starken Passphrase UND einer zweistufigen Verifizierung zu schützen.

Es mag albern klingen, aber mit diese drei einfachen Schritte können Sie sehr erfolgreich Ihren Job, Ihren Ruf und Ihre finanzielle Zukunft schützen.

Gastredakteur

Justin Henderson *(@SecurityMapper) ist Mitbegründer von H & A Security Solutions, zertifizierter Ausbilder im SANS Institut und Autor der "SANS Cyber Defense" und "SIEM" Kurse. Er liebt Cyber Defense und berät auf diesem Gebiet seit fünfzehn Jahren.*

Weiterführende Informationen

Wurde mein Passwort gestohlen?:	https://haveibeenpwned.com/
Zwei-Faktor-Authentifizierung:	https://twofactorauth.org/
NIST SP800-63B Richtlinien für digitale Identitäten:	https://sans.org/for585
Poster: Du bist ein Ziel:	https://www.sans.org/u/OGi