Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

Passwort-Manager

Übersicht

Einer der wichtigsten Schritte sich sicher im Internet zu bewegen ist ein einzigartiges und starkes Passwort für jedes Ihrer Benutzerkonten. Unglücklicherweise haben die meisten von uns Benutzerkonten bei so vielen unterschiedlichen Diensten, dass es fast unmöglich ist, sich all diese Passwörter zu merken. Eine einfache Lösung für dieses Problem ist die Nutzung eines Passwort-Managers, manchmal auch Passwort-Safe genannt. Dieses Programm ist dazu gedacht, all Ihre Zugangsdaten sicher an einer Stelle zu speichern. Zudem bietet es eine Vereinfachung des Anmeldens auf Webseiten, in mobilen Apps und an anderen Applikationen.

Gastautor

Lenny Zeltser legt sein Hauptaugenmerk auf den sicheren Betrieb der IT Systeme von Kunden der NCR Corp. und schult am SANS Institute Spezialisten für IT Sicherheit. Lenny ist auf Twitter als **@lennyzeltser** aktiv und veröffentlicht Artikel auf **zeltser.com**.

Wie funktionieren Passwort-Manager

Passwort-Manager kann man sich als digitalen Tresor vorstellen, man bewahrt seinen Benutzernamen, sein Passwort und andere sensible Informationen sicher darin auf. Wenn Sie sich auf einer Webseite anmelden wollen können Sie sich die Anmeldeinformationen einfach aus dem Passwort-Manager kopieren, manche tun dies sogar automatisch. Dadurch wird es sehr einfach, hunderte einzigartiger, starker Passwörter zu verwenden, da Sie sie sich nicht mehr merken müssen.

Passwort-Manager speichern Ihre Daten in einer Datenbank, die oft auch Tresor oder Safe genannt wird. Dabei werden die Daten in der Datenbank verschlüsselt abgelegt und mit einem Master-Passwort geschützt, das nur Sie kennen. Wenn Sie Daten aus dem Safe benötigen, z.B. um um sich auf der Onlinebanking Webseite Ihrer Bank anzumelden oder um Ihre E-Mails abzurufen, geben Sie einfach nur Ihr Master-Passwort ein, um den Safe zu öffnen.

Einige Passwort-Manager speichern den Passwortsafe lokal auf Ihrem Rechner oder Smartphone, andere hingegen auf einer vom Hersteller des Passwort-Managers betriebenen Webseite. Ergänzend verfügen viele dieser Programme über die Möglichkeit, den Safe automatisch über mehrere, von Ihnen autorisierte, Geräte zu synchronisieren. Wenn Sie also ein Passwort auf Ihrem Laptop aktualisieren, werden diese Änderungen auf Ihr Smartphone, Tablet oder weitere von Ihnen genutzte Computer synchronisiert. Unabhängig vom eigentlichen Speicherort des Safes muss auf allen dieser Geräte der Passwort-Manager installiert sein, um auf diesen zugreifen zu können.

Für die Ersteinrichtung Ihres Passwort-Managers müssen Sie die Anmeldeinformationen und Passwörter von Hand eingeben oder diese importieren. Danach erkennt Ihr Passwort-Manager automatisch, wenn Sie sich bei einem neuen Onlinedienst

Passwort-Manager

registrieren oder das Passwort eines bestehenden Benutzerkontos ändern, und wird die Daten im Safe entsprechend anpassen. Dies ist möglich, weil die meisten Passwort-Manager Hand in Hand mit Ihrem Webbrowser zusammenarbeiten. Diese Integration ermöglicht auch die direkte, automatische Anmeldung an Webseiten.

Passwort-Manager bieten eine einfache Möglichkeit um all Ihre verschiedenen Passwörter sicher zu speichern und zu verwenden.

Passwort-Manager sind so konzipiert, dass sie Ihre sensiblen Daten sicher speichern. Es ist jedoch unabdingbar, Ihr Master-Passwort, das den Inhalt Ihres Passwort-Safes schützt, so zu wählen, dass es stark und schwer zu erraten ist. Daher empfehlen wir ein Passwort zu wählen, welches aus mehreren Wörtern, z.B. einem längeren einprägsamen Satz (engl. passphrase), besteht. Dies stellt aus unserer Sicht eine der sichersten Passwortvarianten dar. Wenn Ihr Passwort-Manager eine Zwei-Wege-Authentifizierung als Anmeldemöglichkeit bietet, sollten Sie diese nutzen. Zu guter Letzt sollten Sie sicherstellen, dass Sie Ihr Master-Passwort für keinen anderen Dienst und auf keinem anderen System benutzen. Wenn Sie diese Ratschläge befolgen, kann ein Angreifer, der in den Besitz des Datensafes Ihres Passwort-Managers gelangt ist, niemals Ihr Passwort erraten und somit keinen Zugriff auf die darin enthaltenen Daten erlangen. Sie sollten sich aber Ihr Master-Passwort gut merken, denn wenn Sie es vergessen, ergeht es Ihnen wie dem Angreifer und Sie haben keinen Zugriff mehr auf Ihre Benutzernamen und Passwörter.

Auswahl eines Passwort-Managers

Es stehen viele kostenlose und kostenpflichtige Passwort-Manager zur Auswahl. Bei der Wahl eines Passwort-Managers, der Ihre Bedürfnisse erfüllen soll, beachten Sie bitte folgendes:

- Stellen Sie sicher, dass er auf allen Plattformen und mobilen Geräten funktioniert von denen Sie auf dessen Passwortsafe zugreifen wollen. Er sollte auch die Möglichkeit bieten den Inhalt des Passwortsafes über all Ihre Geräte zu synchronisieren.
- Benutzen Sie nur weitverbreitete und bekannte Passwort-Manager. Seien Sie vorsichtig, wenn Sie Produkte entdecken, welche erst seit kurzem auf dem Markt sind oder nur einen kleinen oder keinen bekannten Nutzerkreis haben. Genau wie bei gefälschten Virenschutzprogrammen können Cyber-Kriminelle gefälschte Passwort-Manager in Umlauf bringen, die bei Verwendung Ihre Daten stehlen.
- Der gewählte Passwort-Manager sollte zudem einfach bedienbar sein. Wenn Sie finden, dass ein Produkt so kompliziert zu bedienen ist, dass Sie es nicht verstehen, dann suchen Sie eine Alternative die besser zu Ihrer Nutzungsweise und Ihrem Sachverstand passt.

Passwort-Manager

- Die Lösung Ihrer Wahl sollte in stetiger Entwicklung sein und regelmäßig mit Patches versorgt werden. Stellen Sie sicher, dass Sie immer die aktuellste Version nutzen.
- Der Passwort-Manager sollte es Ihnen ermöglichen in wenigen Schritten starke Passwörter für Ihre unterschiedlichen Benutzerkonten zu generieren und die Stärke dieser Passwörter optisch darzustellen.
- Der Passwort-Manager sollte überdies die Möglichkeit bieten zusätzliche sensible Informationen wie z.B. Antworten auf zusätzliche Sicherheitsfragen, Kreditkartendaten oder Informationen über Ihre Vielfliegerkarten zu speichern.
- Nehmen Sie sich in Acht vor Passwort-Managern, welche proprietäre oder unbekannte Verschlüsselungstechniken zur Absicherung Ihres Passwortsafes nutzen. Wenn ein Hersteller damit wirbt, wie er die eigene Verschlüsselungstechnologie entwickelt hat, machen Sie am besten einen großen Bogen um dieses Produkt.
- Vermeiden Sie die Nutzung von Passwort-Managern, welche von sich behaupten in der Lage zu sein, Ihr Master-Passwort wiederherstellen zu können. Das bedeutet, dass die Entwickler der Software Ihr Master-Passwort kennen, was Sie und Ihre Daten einem erhöhten Risiko aussetzt.

Passwort-Manager bieten eine sehr nützliche Unterstützung, um Ihre Passwörter und anderen sensiblen Daten zu schützen. Aber bedenken Sie, dass Sie all diese Informationen an einem Ort speichern. Der Zugriff darauf sollte unbedingt mit einem starken Master-Passwort versehen werden, das nicht nur für Angreifer schwer zu erraten sondern auch für Sie leicht zu merken sein sollte.

Weiterführende Informationen

Starke Passwörter:	http://www.securingthehuman.org/ouch/2015#april2015
Zwei-Faktor-Authentifizierung:	https://www.securingthehuman.org/ouch/2015#september2015
Passwort-Manager:	http://www.computerwoche.de/a/die-besten-passwort-manager,2519783
SANS Sicherheitstip des Tages (engl.):	http://www.sans.org/tip_of_the_day.php

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis