Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Überblick
- Funktionsweise
- Tipps zur Auswahl

Passwortmanager

Überblick

Einer der wichtigsten Schritte den Sie zu Ihrer Absicherung im Internet unternehmen können ist, ein jeweils einzigartiges, starkes Passwort für alle Ihre Benutzerkonten und Apps zu nutzen. Leider ist es sehr wahrscheinlich unmöglich, sich die verschiedenen Passwörter für all Ihre Benutzerkonten zu merken. Aus diesem Grund nutzen so viele Menschen nur ein einziges Passwort für alle Dienste. Dieses Verhalten ist aber gefährlich, denn wenn das Passwort nur bei einem einzigen Dienst in falsche Hände gerät, können Unberechtigte auf alle Dienste zugreifen die das gleiche Benutzerkonto verwenden. Die einfache Lösung hierfür ist ein Passwortmanager, oder auch Passwortsafe genannt. Dabei handelt es sich um Programme, die all Ihre Passwörter sicher speichern, so dass es ein Leichtes ist ein individuelles Passwort für jedes Benutzerkonto zu verwenden. Passwortmanager ersparen Ihnen das Merken vieler Passwörter, stattdessen müssen Sie sich nur das Passwort für den Passwortsafe merken.

Gastautor

Chris Christianson arbeitet seit 20 Jahren als Informationssicherheitsberater in Kalifornien und hält zahlreiche technische Zertifizierungen. Er trat als Sprecher auf einer Vielzahl von Konferenzen auf und trug zu vielen Artikeln dieses Themengebiets bei. Sie erreichen Ihn auf Twitter unter **@cchristianson** und im Web unter **https://ismellpackets.com**.

Funktionsweise

Passwortmanager speichern all Ihre Passwörter in einer Datenbank, auch Safe genannt. Der Passwortmanager verschlüsselt den Inhalt des Safes und schützt ihn mit einem Hauptpasswort, welches nur Sie kennen. Wenn Sie ein Passwort aus dem Safe benötigen, z.B. um sich bei Ihrem Onlinebanking anzumelden, geben Sie einfach Ihr Hauptpasswort ein um den Safe zu entsperren. In vielen Fällen sucht der Passwortmanager das richtige Passwort automatisch heraus und meldet Sie an. So können Sie ganz leicht hunderte von einzigartigen, starken Passwörtern haben, da Sie sich keines davon mehr merken müssen.

Einige Passwortmanager speichern Ihren Safe auf Ihrem Computer oder Mobilgerät, während andere auf Cloud-basierte Speicher setzen. Zusätzlich bieten die meisten Passwortmanager die Möglichkeit, den Passwortsafe auf unterschiedlichen Geräten synchron zu halten. Wenn Sie ein Passwort auf einem Gerät aktualisieren, wird diese Änderung so auch auf allen verknüpften Geräten automatisch verfügbar sein. Unabhängig vom Speicherort des Safes müssen Sie die Passwortmanager-Anwendung auf Ihrem System oder Gerät installieren, um sie zu nutzen.

Passwortmanager

Wenn Sie einen Passwortmanager zum ersten Mal einrichten, müssen Sie all Ihre bestehenden Benutzerkonten manuell importieren oder eingeben. Später kann der Passwortmanager erkennen, wenn Sie sich irgendwo ein neues Benutzerkonto registrieren oder das Passwort eines bestehenden Kontos ändern, und den Passwortsafe entsprechend aktualisieren. Das ist möglich, weil die meisten Passwortmanager Hand in Hand mit Ihrem Browser arbeiten. Diese Integration ermöglicht es auch, dass der Passwortmanager Sie automatisch an Webseiten anmeldet.

Passwortmanager sind eine einfache Möglichkeit, Ihre verschiedenen Passwörter sicher und leicht nutzbar zu speichern.

Es ist unverzichtbar, dass das Hauptpasswort zum Schutz des Passwortsafes sehr stark und unmöglich zu erraten ist. Genau genommen sollten Sie statt eines Passworts sogar einen Passwortsatz nutzen, eine der stärksten Passwortformen. Wenn Ihr Passwortmanager eine zweistufige Anmeldung unterstützt, nutzen Sie das für Ihr Hauptpasswort. Aber vergessen Sie dieses Passwort keinesfalls – ohne dieses Passwort ist der Zugriff auf all die gespeicherten Benutzerkonten unmöglich.

Tipps zur Auswahl

Es gibt viele Passwortmanager, zwischen denen man wählen kann. Die “weiterführenden Informationen” enthalten einen Link mit der Übersicht und Bewertung unterschiedlicher Programme. Beachten Sie bei der Auswahl die folgenden Punkte:

- Der Passwortmanager sollte einfach für Sie zu benutzen sein. Wenn Sie das Programm zu komplex finden, suchen Sie sich besser ein anderes das Ihren Vorstellungen besser entspricht.
- Der Passwortmanager sollte auf allen Geräten funktionieren, auf denen Sie Passwörter nutzen wollen. Es sollte zudem einfach sein, die Passwörter auf allen Geräten synchron zu halten.
- Benutzen Sie nur bekannte und vertrauenswürdige Passwortmanager. Seien Sie vorsichtig bei Produkten, die noch nicht lange auf dem Markt sind oder für die es keine oder wenige Bewertungen im Netz gibt. Vor Herstellern, die damit werben ihre eigenen Verschlüsselungsalgorithmen zu verwenden, sollten Sie ebenso auf der Hut sein.
- Nehmen Sie Abstand von Passwortmanagern, die damit werben ein vergessenes Passwort wiederherstellen zu können. Das bedeutet, dass Ihr Hauptpasswort noch jemandem außer Ihnen bekannt sein muss – ein Risiko das es zu vermeiden gilt.

Passwortmanager

- Stellen Sie sicher, dass – egal welches Produkt Sie wählen – eine fortwährende Wartung durch den Hersteller erfolgt, und nutzen Sie immer die aktuellste Version.
- Ein Passwortmanager sollte eine Möglichkeit zur automatischen Erzeugung von sicheren Passwörtern bieten und die Sicherheit von selbst gewählten Passwörtern bewerten können.
- Der Passwortmanager sollte auch die Möglichkeit bieten, weitere sensible Informationen zu speichern, z.B. die Antworten zu Sicherheitsfragen, Ihre Kreditkartendaten oder die Mitgliedsnummer eines Vielfliegerprogramms.

Passwortmanager sind die wahrscheinlich beste Art, Passwörter und andere kritische Informationen sicher zu speichern. Um so wichtiger ist hierbei die Wahl des Hauptpassworts, um es für Angreifer schwer zu erraten, aber für Sie leicht merkbar zu machen.

Weiterführende Informationen

Die besten Passwortmanager 2017: https://www.computerwoche.de/a/die-besten-passwort-manager,2519783
Passphrasen: https://securingthehuman.sans.org/ouch/2017#april2017
Zwei-Faktor-Authentifizierung: https://www.securingthehuman.org/ouch/2015#september2015
Sichere Passwörter: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
SANS Sicherheitstip des Tages (engl.): https://www.sans.org/tip-of-the-day

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 securingthehuman.sans.org/ouch/archives.

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: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley

