Passwörter verwalten mit dem Passwort-Manager

cebra GmbH - new technologies
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2023-01-04

Vorwort

Sichere Passwörter für alle Onlinekonten sind essenziell. "123456", "hallo" und "Passwort" zählen immer noch zu den am häufigsten vorkommenden Passwort-Kombinationen. Ein Passwort-Manager hilft dabei, verschiedene, komplexe Passwörter zu verwalten.

Die Wichtigsten Informationen rund um Passwort-Manager finden Sie im Folgenden.

Lohnt sich ein Passwort-Manager?

Ja, in der Regel lohnt sich der Einsatz eines Passwort-Managers. Es ist in jedem Fall besser, als gängige Passwörter wiederholt zu benutzen. Die konkrete Entscheidung darüber, welches Programm genutzt wird, erfordert ein individuelles Abwägen der jeweiligen Nutzung. Es geht dabei auch um die Einschätzung des damit verbundenen Risikos.

Wie funktioniert ein Passwort-Manager?

Für einige ist es deswegen eine Strategie, sich ein besonders komplexes Passwort für alle Accounts zu merken. Doch ist dieses einmal geknackt, können Cyber-Kriminelle auf alle sensiblen Daten zugreifen. Am sichersten ist es aus diesem Grund, für jeden Account ein eigenes, komplexes Passwort zu haben – wenngleich das bedeutet, mehrere Dutzend von Zugangsdaten zu verwalten. Wer da den Überblick verliert, für den kann ein Passwort-Manager Abhilfe schaffen.

Checkliste:

- Von E-Mail bis Social Media: Für welche Konten brauchen Sie einen Passwort-Manager?
- Browser-basiert oder eigenständig: Welches Programm passt am besten zu Ihren Online-Gewohnheiten?
- Cloud oder Festplatte: Wo werden Ihre Daten gesichert?
- Sensible Daten: Benötigen Sie einen zweiten Faktor zur Authentisierung?
- Komplexe Kombinationen: Haben Sie ein sicheres Masterpasswort?

Passwort-Manager sind Programme, die Benutzernamen und Passwörter verwalten. Mittels Verschlüsselung und eines komplexen Masterpassworts verwahren Passwort-Manager die Passwörter sicher. Sie funktionieren ähnlich wie ein Notizbuch, das in einer Schublade eingeschlossen ist und dessen Inhalte somit nur für den Besitzer oder die Besitzerin einsehbar sind. Der Vorteil liegt auf der Hand: Anstelle von vielen verschiedenen Passwörtern muss sich nur noch eins gemerkt werden.

Vorteile des Passwort-Managers

- **Verwahren von Passwörtern** und Benutzernamen mittels Verschlüsselung
- **Unterstützung bei der Passwortvergabe**: z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.
- **Warnung vor gefährdeten Websites und möglichen Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.
- **Synchronisieren möglich:** Wer Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen nutzen möchte, kann ein Programm verwenden, das diese synchronisiert.

Passwörter mit dem Passwort-Manager speichern

Je nach Wahl des Programms werden die Passwörter entweder lokal auf dem Gerät oder zwecks Synchronisierung auf verschiedene Systeme auch in der Infrastruktur des Anbieters – oftmals cloudbasiert – gespeichert.

Eigenständiges Passwort-Manager-Programm
Sind eigenständige Programme einmal aktiviert und eingerichtet, erscheint ein Pop-up-Fenster, wenn zur Nutzung eines Online-Dienstes die Eingabe von Nutzernamen und Passwort erforderlich sind. Dann muss ein zentral hinterlegtes Masterpasswort eingegeben werden, das alle Zugangsdaten schützt.

Im Browser integrierte Passwort-Manager
Viele Webbrowser bieten bereits einen integrierten Passwort-Manager an, der ohne großen Aufwand genutzt werden kann. Einmal eingerichtet, agiert er eigenständig und das Programm wird beim Aufrufen einer Website aktiv, sofern dort Zugangsdaten benötigt werden. Da Browser aber komplexe Programme sind, die dieses Thema nicht mit oberster Priorität behandeln, können die Zugangsdaten relativ einfach von Schadsoftware extrahiert und somit von einem Angreifer missbraucht werden.

Die Verwendung eines Masterpassworts bietet zwar ein Mindestmaß an Schutz, doch Anwender und Anwenderinnen sollten immer die neuesten Updates durchführen. Außerdem sollte der Zugang zum Computer, Tablet oder Smartphone gesichert werden, z. B. durch eine PIN- oder Passwort-Abfrage.

Nachteile des Passwort-Managers

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Alle Passwörter können auf einmal gestohlen werden, sollte ein Cyber-Angriff auf einen Passwort-Manager erfolgreich sein.
- Bei cloudbasierten Diensten vertrauen Sie den Zugang zu all Ihren sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind.

Passwörter speichern - Multifaktorauthentifizierung

Für Ihre hochsensiblen Inhalte sollten Sie im Passwort-Manager am besten einen erweiterten Schutz einrichten. Dieser lässt sich durch die Einrichtung eines zweiten Faktors bei wichtigen Accounts realisieren. Dann könnte zum Beispiel ein Bestätigungscode an ein weiteres Gerät wie Ihr Smartphone gesendet werden, um den Vorgang eindeutig zu authentisieren. Zu den wichtigen Accounts gehören beispielsweise Ihre E-Mail-Konten. Denn wenn Dritte Zugang dazu erhalten,

können diese deutlich größeren Schaden anrichten. Einerseits könnten sie auf Ihre E-Mail-Daten zugreifen, darüber hinaus auch in Ihrem Namen Nachrichten versenden. Zudem können Cyber-Kriminelle mit Zugriff auf Ihr E-Mail-Konto weitere Online-Dienste übernehmen, indem sie Passwörter darüber zurücksetzen.

Revision #1
Created 4 January 2023 14:37:01 by Christian Sigl
Updated 4 January 2023 14:42:42 by Christian Sigl