Passwort-Manager

Info

Der Passwortmanager ist das essenzielle Tool, um den nötigen Sicherheitsvorkehrungen bezüglich sicherer Passwörter gerecht zu werden. Hier kannst du dir anschauen, was gute Passwörter sind und wie wir damit umgehen sollten: Gegenmaßname Passwörter

KeePassXC und Bitwarden sind beide Open-Source und haben Anwendungen für alle üblichen Betriebssysteme / Browser.

KeePassXC funktioniert Offline, Bitwarden online. Aber auch KeePassXC lässt sich mittels externer Dienste über mehrere Geräte synchronisieren.

Praktikable Passwortmanager für PCs:

- KeePassXC: Linux, Windows, MacOS
- Bitwarden: Linux, Windows, MacOS

KeePass für Mobilgeräte

Empfehlung aus KeePassXC docs für Handys:

- Android: keepassDX, Keepass2Android
- iOS: Strongbox, KeePassium

Die in Browser und Betriebssysteme integrierten Passwortmanager sind nicht unbedingt zu empfehlen, da diese oftmals proprietär und überwiegend auf Komfort ausgelegt sind. Das führt regelmäßig zu Sicherheitslücken. Besonders Browser sind stets im Fokus von Angreifer*innen und bieten viele Angriffsvektoren.

KeePassXC

KeePassXC ist einer der bekanntesten und verbreitetsten Passwortmanager. Er ist Open-Source, wird regelmäßig durch Expert*innen auf Schwachstellen untersucht und bietet eine Vielzahl von sehr praktischen Features. Diese ermöglichen es uns die Lücke zwischen Sicherheit und Komfort zu

schließen.

Browserintegration

Es gibt für alle gängigen Browser *(außer Safari*) eigene Plugins für KeePassXC, um die auto-fill Funktion komfortabel nutzen zu können. Damit werden auf jeder Webseite, für die Passwörter gespeichert wurden, automatisch die richtigen Login-Daten vorgeschlagen.

Das verhindert, dass Du, wenn du auf einen Phishing-Link klickst, aus Versehen dein Passwort eingibst, weil das Plugin merkt, dass Du auf einer falschen URL gelandet bist.

Schlüsseldatei

Es empfiehlt sich eine Passwortdatenbank sowohl mit Passwort, als auch mit einem zweiten Faktor abzusichern. Die einfachste Methode dafür ist die Schlüsseldatei *(eng:Key-File). (Weiter unten gibt es ein Beispiel Szenario.)*

Im folgenden sind verschiedene Methoden aufgelistet, wie die Schlüsseldatei als zweiter Faktor genutzt werden kann.

Schlüsseldatei als 2. Faktor

Es gibt die Möglichkeit, die Datenbank neben dem Passwort zusätzlich noch mit einer separaten Schlüsseldatei zu verschlüsseln. Das heißt man braucht dann, um an die Passwörter zu kommen, immer sowohl das Passwort, als auch die Schlüsseldatei.

Eine Anleitung dazu findest du hier.

Schlüsseldatei als Hauptschlüssel

Du kannst deine Passwortdatenbank auch nur mit einer Schlüsseldatei verschlüsseln, ohne Passwort. Dann musst du beim öffnen der Datenbank in KeePassXC immer die Schlüsseldatei auswählen.

Schlüsseldatei als Hauptschlüssel mit 2. Faktor Passwort

Ein häufiger Anwendungsfall dafür ist das Speichern der Schlüsseldatei auf einem verschlüsselten USB-Stick, den zB an deinem Schlüsselbund, immer mit sich geführt wird.

Auch damit ist eine 2-Faktor-Authentifizierung gewehrleistet. Es wird:

1. Faktor: das Passwort für den Stick
2. Faktor: der Stick (mit der Schlüsseldatei)

benötigt, um an die Passwörter zu kommen. Dabei muss unbedingt drauf geachtet werden, das es einen Backup-USB-Stick gibt, falls der eigentliche Stick mal verloren geht!

Neue Passwörter generieren

Eines der Kernfeatures eines Passwortmanagers ist, dass die starke Passwörter oder Passphrasen nach euren eigenen Vorgaben generieren können. Damit ist sichergestellt, dass ihr nicht doch aus Bequemlichkeit immer das gleiche Passwort wiederverwendet.

Passwörter in der Cloud synchronisieren und backupen

Ist das nicht gefährlich?

Die Passwortdatenbank ist immer, zu jeder Zeit verschlüsselt. Sie wird zu keiner Zeit in der Cloud entschlüsselt, sodass die Cloud-Betreiber etwas daraus lesen könnten.

Allerdings könnte die Polizei eventuell eine Kopie deiner Datenbank klauen wie im folgenden Beispiel Szenario beschrieben.

Beispiel-Szenario

Nehmen wir an, deine Passwortdatenbank ist "nur" mit einem (starken) Passwort geschützt. Hat nun die Polizei Zugriff auf deine Cloud (oder kommt anderweitig an deine Datenbank), hat sie nur die verschlüsselte Datei erbeutet und kann damit erst mal nichts anfangen. Sollten sie aber in Zukunft dein Passwort auf irgendeine Art erfahren (sie beobachten Dich zB heimlich, wie du es eintippst), dann können sie die verschlüsselte Datenbank wieder rausholen und jetzt entschlüsseln.

Wäre die Datenbank zusätzlich mit einer Schlüsseldatei verschlüsselt, reicht es nicht aus, nur das Passwort zu kennen, sondern es braucht auch die Schlüsseldatei. Würdest du diese Schlüsseldatei nun zerstören, gäbe es keinerlei Möglichkeit mehr, die geklaute Datenbank jemals zu entschlüsseln.

How To

Du könntest zum Beispiel deine Datenbank seelenruhig in der Cloud lagern und somit auch gleichzeitig mit all deinen Geräten darauf zugreifen.

Die Schlüsseldatei hast du jeweils **nur lokal** auf deinen Geräten gespeichert.

Falls du jetzt einmal den Verdacht bekommen solltest, dass die Behörden eine Kopie deiner Passwortdatenbank bekommen haben

1. machst Du eine Kopie deiner Datenbank

2. erstellst dafür sowohl ein neues Passwort,
3. als auch eine neue Schlüsseldatei
4. und kannst danach die **alte Schlüsseldatei** auf alle deinen Geräten löschen.

Damit ist die kompromittierte Datenbank für immer nutzlos.

Achtung
Bevor du deine alte Schlüsseldatei löschst, stelle sicher: 1. dass die neue Datenbank mit der neuen Schlüsseldatei funktioniert 2. Du das neue Passwort nicht direkt vergisst!

In beiden Fällen wären all deine Passwörter unwiederbringlich weg.

KeePassXC als 2-Faktor-App

KeePassXC kann auch als 2FA-App mit TOTP genutzt werden. Das funktioniert sogar auf den Apps für Handy.

Anleitung

Hier findet sich eine Anleitung mit weiteren Verweisen.

Hinweis

Wir schreiben hier konsistent von KeePassXC.

Ältere Versionen wieKeePassX und KeePass sollten nicht mehr benutzt werden.

Version #3
Erstellt: 14 Januar 2025 19:53:19 von ESC-IT Migration Bot
Zuletzt aktualisiert: 11 Februar 2025 14:17:52 von ESC-IT Migration Bot