DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung KeepassXC

KeePassXC: Auto-Type und Browser-Add-on im Alltag nutzen – Passwörter Teil1

1. Passwort-Management

Unsichere oder mehrfach verwendete Passwörter sind oftmals ein Einfallstor für Datenmissbrauch und -diebstahl. Daher ist es ratsam, für jeden Online-Dienst ein **unterschiedliches** Passwort zu verwenden. Gleichzeitig gilt allerdings auch, dass Passwörter komplex, ausreichend lang und insbesondere zufällig sein sollten, um einen Schutz zu bieten. In der Praxis stoßen wir hier unweigerlich auf ein Problem: Wer soll sich diese Passwörter alle merken? Bei durchschnittlich über 20 Online-Accounts, die jeder von uns besitzt, ist das nicht zu schaffen. Daher ist es sinnvoll einen Passwort-Manager zu verwenden, der uns diese Aufgabe abnimmt.

Passwort-Manager verwalten bzw. speichern die verschiedenen Passwörter zu den Online-Accounts in einer verschlüsselten Datenbank. Über ein sogenanntes **Master-Passwort** wird der Zugang zu dieser Datenbank geschützt. Nach der Eingabe des korrekten Master-Passworts hat man Zugriff auf alle gespeicherten Passwörter – vor diesem Hintergrund ist es essenziell, ein Master-Passwort zu wählen, das wirklich »sicher« ist. Mit dem Diceware-Verfahren (erklärt ab Ziffer 5.) könnt ihr euch ein solches Passwort bzw. Passphrase »würfeln«. Der Vorteil dieses Verfahrens liegt auf der Hand: Ihr erhaltet nicht nur ein **sicheres** Passwort, sondern auch eines, das ihr euch merken könnt.

Mit der dreiteiligen Artikelserie »Passwörter« möchte ich euch konkrete Tipps für KeePassXC (Desktop) und KeePassDX (Android) an die Hand geben, die euch die Nutzung bzw. den Umgang mit Login-Daten im Alltag erleichtern. Die Synchronisation der Passwort-Datenbank werde ich im dritten Teil der Serie am Beispiel von Syncthing erläutern.

Dieser Beitrag ist Teil einer Artikelserie:

- KeePassXC: Auto-Type und Browser-Add-on im Alltag nutzen – Passwörter Teil1
- KeePassDX: Magikeyboard und AutoFill im Android-Alltag nutzen – Passwörter Teil2
- Syncthing: KeePass-Datenbank zwischen PC und Android synchronisieren – Passwörter Teil3

2. Passwort-Manager

Passwörter sind ein **ständiger** Begleiter des Alltags. Wir entsperren damit unseren Rechner oder das Smartphone, loggen uns in das Bankkonto ein oder authentisieren uns damit bei einem der zahllosen Online-Dienste, die wir nutzen. Es ist daher essenziell sich eingehend mit dem Thema Passwort zu befassen, da wir darüber unsere (digitale) Identität bzw. Online-Konten schützen.

Im Beitrag »Sicheres Passwort wählen: Der Zufall entscheidet« hatte ich aufgezeigt, wie wichtig es ist, für jeden Online-Dienst ein unterschiedliches, ausreichend langes und insbesondere zufälliges Passwort zu wählen. Ein Passwort-Manager ist dabei das zentrale Element bei der Generierung, Speicherung und Verwaltung von Passwörtern. Eine kurze Zusammenfassung des Beitrags:

- Es ist empfehlenswert einen Passwort-Manager zu nutzen, der zufällige Passwörter generieren und speichern kann. Dafür eignet sich bspw. das Tool KeePassXC – verfügbar für Windows, macOS und GNU/Linux und KeePassDX für Android. Grundsätzlich solltet ihr davon absehen, eure Passwörter online in einer »Cloud« abzulegen. Passwörter gehören nicht in fremde Hände. (LastPass-Hack, OneLogin-Hack, 1Password Daten-Leak)
- Wer sich für die Nutzung eines Passwort-Managers entscheidet, der sollte allerdings bedenken, dass dieser sensible Passwörter beinhaltet. Das bedeutet: All eure Passwörter sind an einem Ort versammelt und lassen sich einsehen, falls sich jemand Zugriff zu eurem Passwort-Manager verschafft. Daher solltet ihr den Zugang zum Passwort-Manager mit einem Passwort sichern, das folgende Kriterien erfüllt:
  - Zufällig
  - Leicht zu merken
  - Lang genug, um gegen Brute-Force oder Combinator-Angriffe zu bestehen

  Solch ein Passwort bzw. Passphrase könnt ihr bspw. über das Diceware-Verfahren erstellen.

Der Grundstein ist hiermit gelegt. Damit die Nutzung im Alltag gelingt, sollte man ein paar Hinweise und Tipps kennen, die den Umgang mit einem Passwort-Manager vereinfachen können und für mehr Sicherheit sorgen. Ein paar dieser Tipps werde ich im Rahmen der Artikelserie vorstellen.

Hinweis

Eine ausführliche Beschreibung für die Einrichtung eines Passwort-Managers, die Generierung von sicheren Passwörtern und weitere Hintergrundinformationen wie dem Diceware-Verfahren findet ihr im Beitrag »Sicheres Passwort wählen: Der Zufall entscheidet«.

3. KeePassXC

Zu KeePass gibt es unterschiedliche Implementierungen für verschiedene Plattformen. Die dabei verwendeten Datenbanken sind üblicherweise kompatibel. Das bedeutet: Die Passwort-Datenbanken können mit verschiedenen Methoden (bspw. Syncthing) zwischen den Geräten synchronisiert werden.

Für den Desktop halte ich KeePassXC für empfehlenswert, da es plattformübergreifend zur Verfügung steht, aktiv entwickelt wird und neue (Sicherheits-)Funktionen implementiert. Die nachfolgende Beschreibung richtet sich daher primär an Nutzer von KeePassXC – kann aber auch mit anderen Varianten bzw. Versionen von KeePass kompatibel sein.

Passwort-Manager sollen die Verwaltung und auch Nutzung von Login-Daten im Alltag vereinfachen. Anstatt die Passwörter für einen Online-Account umständlich zwischen Passwort-Datenbank und einer Webseite hin- und herzukopieren, gibt es komfortablere und weniger fehleranfällige Verfahren wie Auto-Type und Browser-Add-ons. Beide Varianten möchte ich euch nachfolgend vorstellen.

4. Auto-Type

KeePassXC ist standardmäßig so eingestellt, dass man Passwörter mit der Tastenkombination `STRG + ALT + A` automatisch in Formularfelder einer Webseite einfügen lassen kann. Diese Auto-Type-Funktion hat einen entscheidenden Vorteil gegenüber dem simplen hin- und herkopieren von sensiblen Informationen via `STRG + C` und `STRG + V`, bei der sowohl Nutzername als auch Passwort im Zwischenspeicher (Zwischenablage) eures Systems landen. Diese Zwischenablage (engl. Clipboard) ist kein sicherer Ort, um euer Passwort »zwischenzuspeichern«.

Mit der Auto-Type-Funktion könnt ihr diese Problematik umgehen. Bei dieser Variante wird das Passwort nicht in die Zwischenablage kopiert, sondern direkt zwischen KeePassXC und dem Browserfenster ausgetauscht – es werden simulierte Tastendrücke direkt in das Eingabefeld (Login / Passwort) gesendet. Der Mittelsmann (die Zwischenablage) wird dabei also umgangen bzw. ist nicht mehr erforderlich. Auto-Type überträgt eure Login-Daten also direkt in die dafür notwendigen Felder. Das spart Zeit und erhöht die Sicherheit.

Damit Auto-Type auch funktioniert, muss Folgendes erfüllt sein:

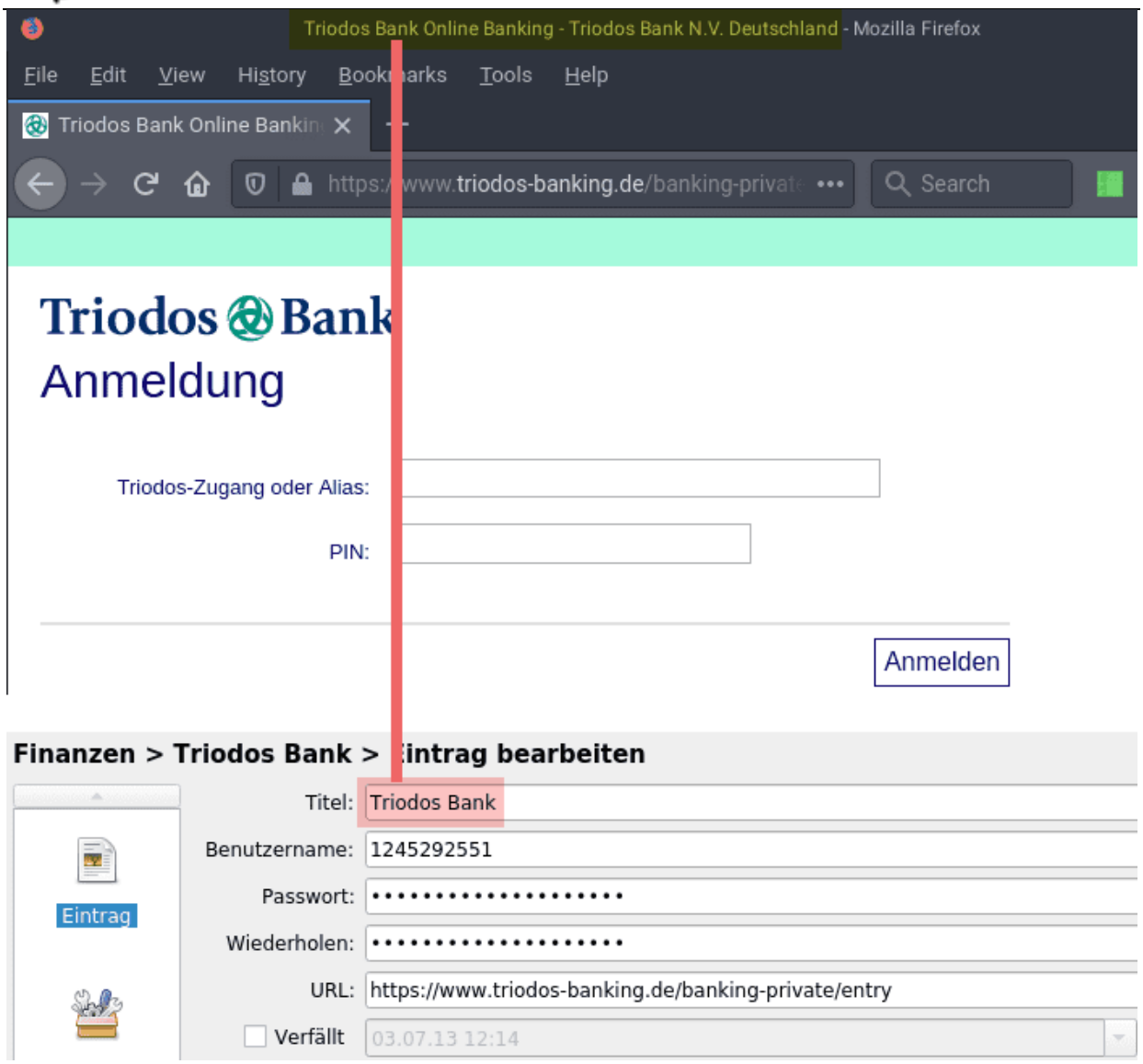
- Die KeePassXC-Datenbank muss entsperrt sein. Ist sie gesperrt erscheint beim Drücken der Tastenkombination die Passwortabfrage
- Benutzername und Passwort für den entsprechenden Login bzw. Webseite müssen hinterlegt sein
- Der Titel des Eintrags in der KeePassXC-Datenbank sollte Ähnlichkeit mit dem Titel des Browser-Fensters bzw. der Seite haben, bei der ihr euch einloggen wollt

Sind diese Anforderungen erfüllt, orientiert sich die Auto-Type-Funktion am `Titel` des Eintrags, den ihr in KeePassXC hinterlegt habt und gleicht diesen mit dem Titel des Browser-Fensters ab. Drückt ihr **innerhalb eines Browser-Fensters** dann die Tastenkombination `STRG + ALT + A` wird Auto-Type versuchen einen passenden Eintrag in eurer KeePassXC-Datenbank zu ermitteln. Dieser Schritt ist erforderlich, damit Auto-Type weiß, welche Login-Daten auf einer bestimmten Seite eingetragen werden sollen.

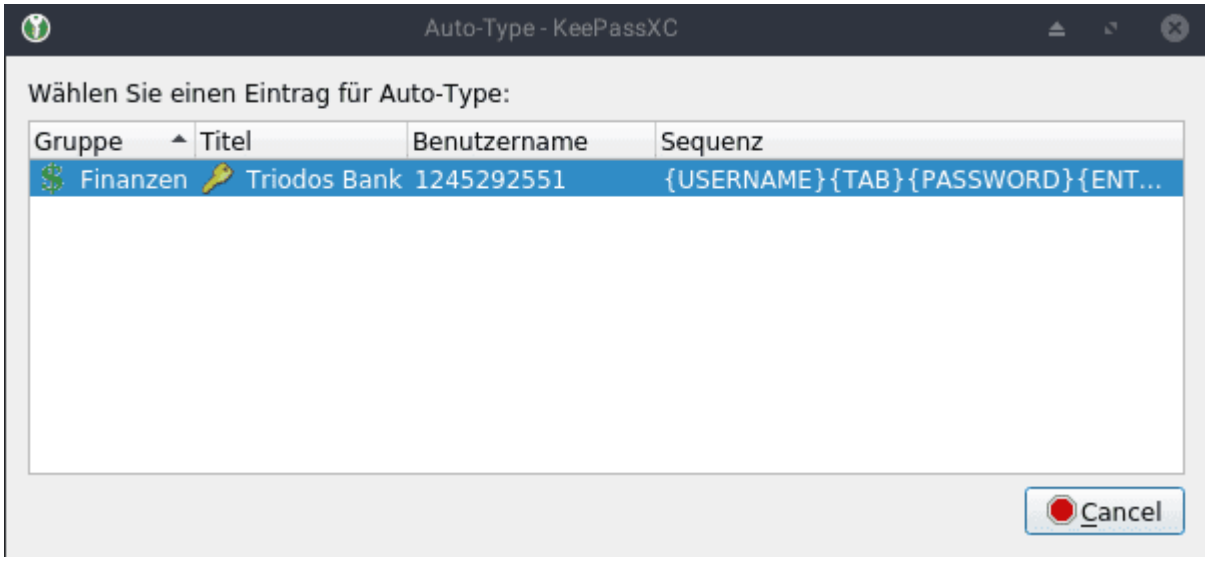
Die Tastenkombination für das Auto-Type kann über `Werkzeuge -> Einstellungen -> Allgemein -> Auto-Type -> Globale Tastenkombination für Auto-Type` angepasst werden. Bei manchen Systemen ist die Standardeinstellung `STRG + ALT + A` bereits anderweitig belegt.

4.1 Anmeldung via Auto-Type

Anhand eines Beispieles lässt sich das gut verdeutlichen. Angenommen jemand möchte sich bei der Triodos Bank mittels Auto-Type-Funktion anmelden, dann gleicht Auto-Type nach Absenden der Tastenkombination `STRG + ALT + A` den Titel des Browserfensters mit den in KeePassXC hinterlegten Einträgen ab:

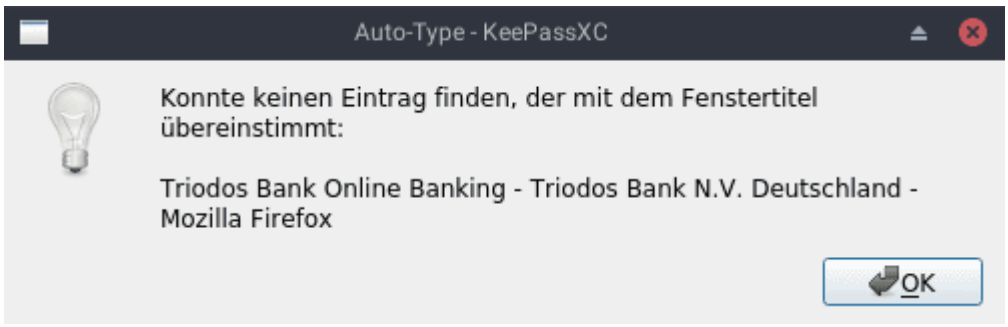


Kommt es zu einer Übereinstimmung bzw. Ähnlichkeit wird euch KeePassXC einen Vorschlag unterbreiten, den ihr mit einem Klick bestätigen müsst:

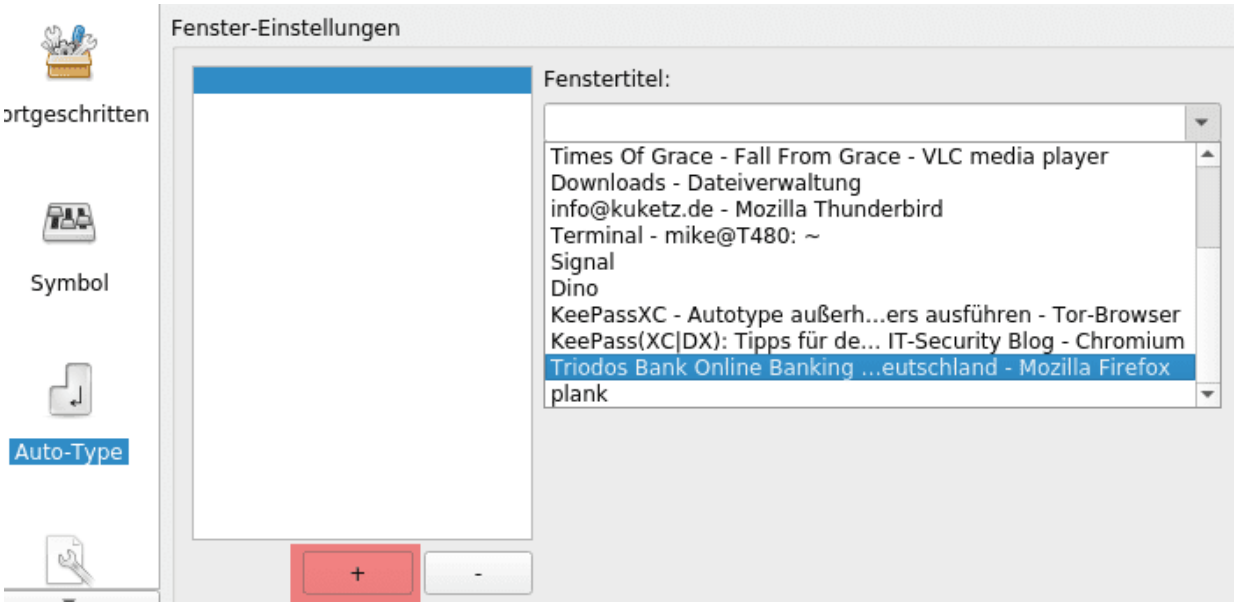


4.2 Keine Übereinstimmung

Findet KeePassXC keine Übereinstimmung, wird euch ein Hinweis eingeblendet:



Ihr könnt nun entweder den Titel des Eintrags in KeePassXC anpassen oder den Fensternamen des Browsers fest dem Eintrag zuweisen. Dazu klickt ihr innerhalb eines Eintrags auf `Auto-Type` und nehmt über das `Plus-Zeichen` eine feste Zuweisung zu einem Fenster zu:



Insgesamt ist die Auto-Type-Funktion eine relativ sichere und komfortable Möglichkeit, um sich online in ein Konto einzuloggen. Je nach System, Browser und auch Härtungsgrad des Systems treten bei dieser Variante allerdings gerne mal kleine Fehler auf, die das Übertragen von Anmeldedaten zu einem Geduldsspiel werden lassen. Weniger fehleranfällig ist die Verwendung eines Browser-Add-ons.

Hinweis

Weitere Informationen zu Auto-Type findet ihr im offiziellen KeePassXC-Wiki.

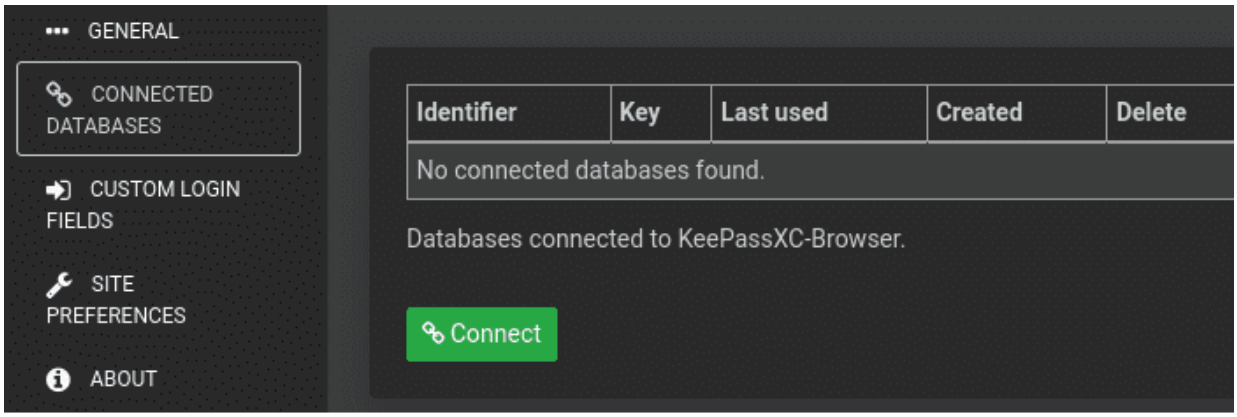
5. Browser-Add-on: KeePassXC-Browser

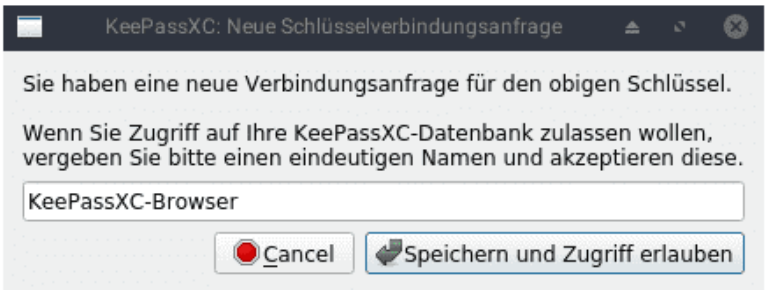
Eine Alternative zur Auto-Type-Funktion ist die Installation eines Browser-Add-ons. Das KeePassXC-Projekt bietet ein offizielles Add-on für Firefox, Chrome etc. an. Am Beispiel von Firefox möchte ich nachfolgend auf das Add-on eingehen.

5.1 Installation und Anbindung

Vor der Installation des Add-ons muss die Browser-Integration innerhalb KeePassXC zunächst über `Werkzeuge -> Einstellungen -> Browser-Integration` aktiviert werden. Setzt ein Häkchen bei `KeePassXC-Browser-Integration` aktivieren und anschließend noch für jene Browser, mit denen ihr das Add-on verwenden wollt.

Anschließend erfolgt die Installation des Firefox-Add-ons über die Mozilla-Webseite. Dort ist das Add-on unter dem Namen KeePassXC-Browser zu finden. Nach erfolgter Installation muss zunächst eine Verbindung zur KeePassXC-Datenbank hergestellt werden. Dazu öffnet man die Einstellungen des Add-ons und navigiert zu »Connected Databases« und fügt über den Button `Connect` eine Datenbank hinzu. Die Verbindungsanfrage zur Datenbank bzw. der Zugriff darauf muss anschließend noch erlaubt werden:





5.2 Anmeldung via Add-on

Damit ist die Verbindung zur KeePassXC-Datenbank hergestellt. Ähnlich wie beim Auto-Type-Verfahren wird KeePassXC anhand der hinterlegten Titel prüfen, ob die Login-Daten für eine Webseite infrage kommen. Wird ein Eintrag gefunden, der eine Übereinstimmung hat, fragt KeePassXC, ob ein Zugriff auf den Eintrag durch das Add-on erfolgen darf – dies kann man einmalig oder dauerhaft erlauben:

5.3 Erhöhte Angriffsfläche

Im Zusammenhang mit dem Add-on wirft sich unweigerlich die Frage auf, ob dies hinsichtlich der Sicherheit nicht ein Risiko darstellt bzw. die Angriffsfläche erhöht. Denn Browser sind oftmals von Sicherheitslücken betroffen, die unter Umständen dazu ausgenutzt werden könnten, um sich Zugang zu den Passwörtern in KeePassXC zu verschaffen. Von den schadhaften Add-ons ganz zu schweigen.

Im Vergleich zum Auto-Type-Verfahren ist dieser Ansatz tatsächlich mit einem höheren Risiko behaftet. Verschiedene Sicherheitsmaßnahmen minimieren das Risiko allerdings. So nutzt KeePassXC zur Übermittlung von Passwörtern zwischen Add-on und der Datenbank bspw. eine verschlüsselte Verbindung (via TweetNaCl.js), die über ein Public-Key-Verfahren authentifiziert wird. Das ältere TCP-Socket-basierte KeePassHTTP wurde also durch ein natives, verschlüsseltes Messaging ersetzt, um sicherzustellen, dass KeePassXC-Browser nur mit einer bestimmten Anwendung kommunizieren kann. Weiterhin gilt:

- Die KeePassXC-Datenbank muss offen sein, damit das Add-on Passwörter abrufen kann
- Zu keinem Zeitpunkt besteht Zugriff auf das Masster-Passwort der Datenbank
- Vor dem Zugriff auf Anmeldedaten muss dies durch den Nutzer bestätigt werden

Haltet ihr euch zusätzlich an die nachfolgenden Tipps, ist das Risiko eines unautorisierten Zugriffs auf die KeePassXC-Datenbank als sehr gering einzuschätzen:

- **Updates**: Haltet euren Browser stets aktuell bzw. spielt regelmäßig (System-)Updates ein
- **Vertrauenswürdige Add-ons**: Installiert euch nur vertrauenswürdige Add-ons, wie sie bspw. im Firefox-Kompendium vorgestellt werden
- **Beschränkte Nutzung**: Nutzt den Browser ausschließlich zum Einloggen in eure Online-Konten (nach dem 3-Browser-Konzept)

Als zusätzliche Maßnahme kann man auch zwei verschiedene Passwort-Datenbanken anlegen. Eine Datenbank mit eher unkritischen Zugangsdaten und eine weitere mit den sensiblen Zugangsdaten wie für Banken etc. Dem Add-on kann im Anschluss nur auf die eher unkritische Datenbank Zugriff gewährt werden.

Hinweis

Weitere Informationen zum Browser-Add-on findet ihr im offiziellen KeePassXC-Wiki.

6. Fazit

Anstatt die Passwörter für einen Online-Account umständlich zwischen Passwort-Datenbank und einer Webseite hin- und herzukopieren, solltet ihr das Auto-Type-Verfahren verwenden. Funktioniert die Auto-Type-Funktion bei eurem Setup nicht korrekt, kann das Browser-Add-on Abhilfe schaffen. Allerdings solltet ihr euch hier dem erhöhten Risiko bewusst sein und die Tipps berücksichtigen, um eure Anmeldedaten nicht unnötig zu gefährden.

Im folgenden Teil der Artikelserie werde ich das Magikeyboard und die AutoFill-Funktion von KeePassDX (Android) vorstellen. Ähnlich wie bei Auto-Type-Verfahren ist damit die komfortable und auch sichere Übertragung von sensiblen Anmeldedaten in andere Apps wie bspw. dem Browser möglich.

Quelle: https://www.kuketz-blog.de/keepassxc-auto-type-und-browser-add-on-im-alltag-nutzen-passwoerter-teil1/