Passwortverwaltung

Da für jeden Dienst ein anderes Passwort verwendet werden sollte, ist ein Programm zur Verwaltung hilfreich: **KeePassXC** ist *freie Software* und speichert zusätzliche Informationen und Passwörter verschlüsselt mit einem Masterpasswort.

Schritt 1: Software installieren

KeePassXC kann unter https://keepassxc.org/download/ für Linux, Mac und Windows heruntergeladen werden.

Schritt 2: Sprache ändern

Sollte die Oberfläche von KeePassXC englisch sein, kann dies wie folgt geändert werden:

- Menüleiste ***Tools*** (Werkzeuge)→ ***Preferences*** (Einstellungen) → ***Language*** (Sprache)

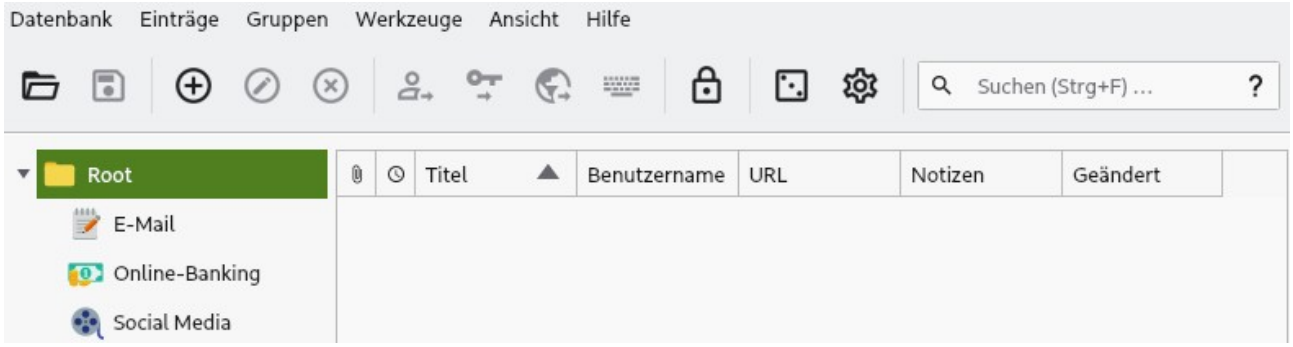
Schritt 3: Neue Passwort-Datenbank erstellen

- Menüleiste ***Datenbank → Neue Datenbank***
- Masterpasswort setzen und wiederholen (Eine nachträgliche Änderung ist möglich)

Die **Passwort-Datenbank** ist eine **sehr wichtige Datei mit der Endung „.kdbx“**. Die Passwörter werden verschlüsselt in dieser Datei/Datenbank gespeichert, weshalb sie nur schwer rekonstruierbar sind. Diese Datenbank sollte daher weder entschlüsselt werden können, noch verloren gehen. Deshalb ist es extrem wichtig,

> *1. dass das **Masterpasswort sicher und gut merkbar** ist – **davon hängt die Sicherheit aller weiteren Passwörter ab** (→ mehr zu Passwörtern bei Schritt 6).*
>
> *2. dass **regelmäßig Datensicherungen (Backups)** gemacht werden.*

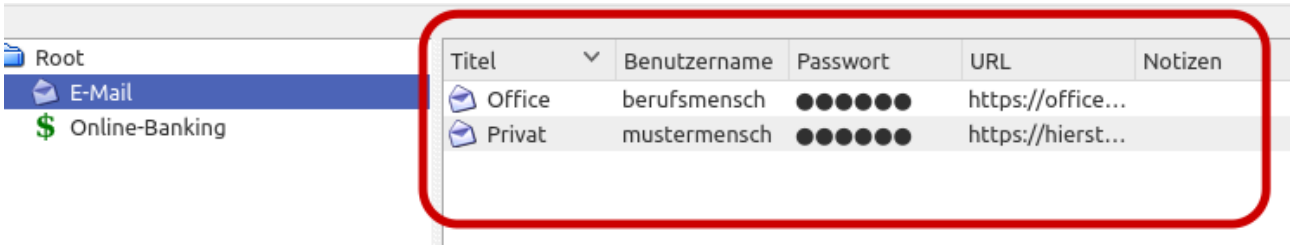
Schritt 4: Passworteinträge erstellen



Wenn das Hauptpasswort erfolgreich eingegeben wurde, öffnet sich die Datenbank. Direkt nach Erstellung sind keine Einträge (linke Seite) vorhanden.

Nun können im linken Bereich **[1]** Gruppen erstellt und geordnet werden. Jede Gruppe kann eine Vielzahl an Passworteinträgen enthalten. Diese werden über einen Linksklick auf den gelben Schlüssel mit grünen Pfeil **[2]** unterhalb der Menüleiste erstellt. Alternativ ist das Anlegen eines neuen Eintrags auch via Rechtsklick im rechten Bereich des Programms möglich.

Mit einem Linksklick kann die entsprechende Gruppe ausgewählt werden. In dieser können dann – wiederum mit einem Linksklick auf den gelben Schlüssel mit grünem Pfeil **[2]**, alternativ per Rechtsklick – die einzelnen Einträge zu den Passwörtern angelegt werden.



Wie immer gilt: Nachdem Änderungen vorgenommen wurden, muss die Passwort-Datenbank erneut gespeichert werden (Diskettensymbol [3]). Sonst gehen die Änderungen beim Schließen des Programms verloren.

Alternativ kann die Einstellung „automatisch speichern“ aktiviert werden:

- Menüleiste ***Werkzeuge → Allgemein → Automatisch nach jeder Änderung speichern***

Schritt 5: Passwörter verwenden

Ein in der Übersicht markiertes Passwort kann mittels „Kopieren“ und „Einfügen“ (Strg+C und Strg+V) für kurze Zeit in die Zwischenablage kopiert und anschließend eingefügt werden. Allerdings landen beim Kopieren (Strg+C) die sensiblen Daten zunächst in einem Zwischenspeicher (sog. Zwischenablage) auf dem Computer. **Dies ist kein sicherer Ort, da bösartige Software die Zwischenablage auslesen und den Inhalt an Dritte über-**

mitteln könnte. Die Zwischenablage wird nach einer Weile von KeePassXC zwar wieder gelöscht, dennoch ist dieses kein Schutz gegen ein automatisiertes Auslesen (z.B. durch Schadsoftware).

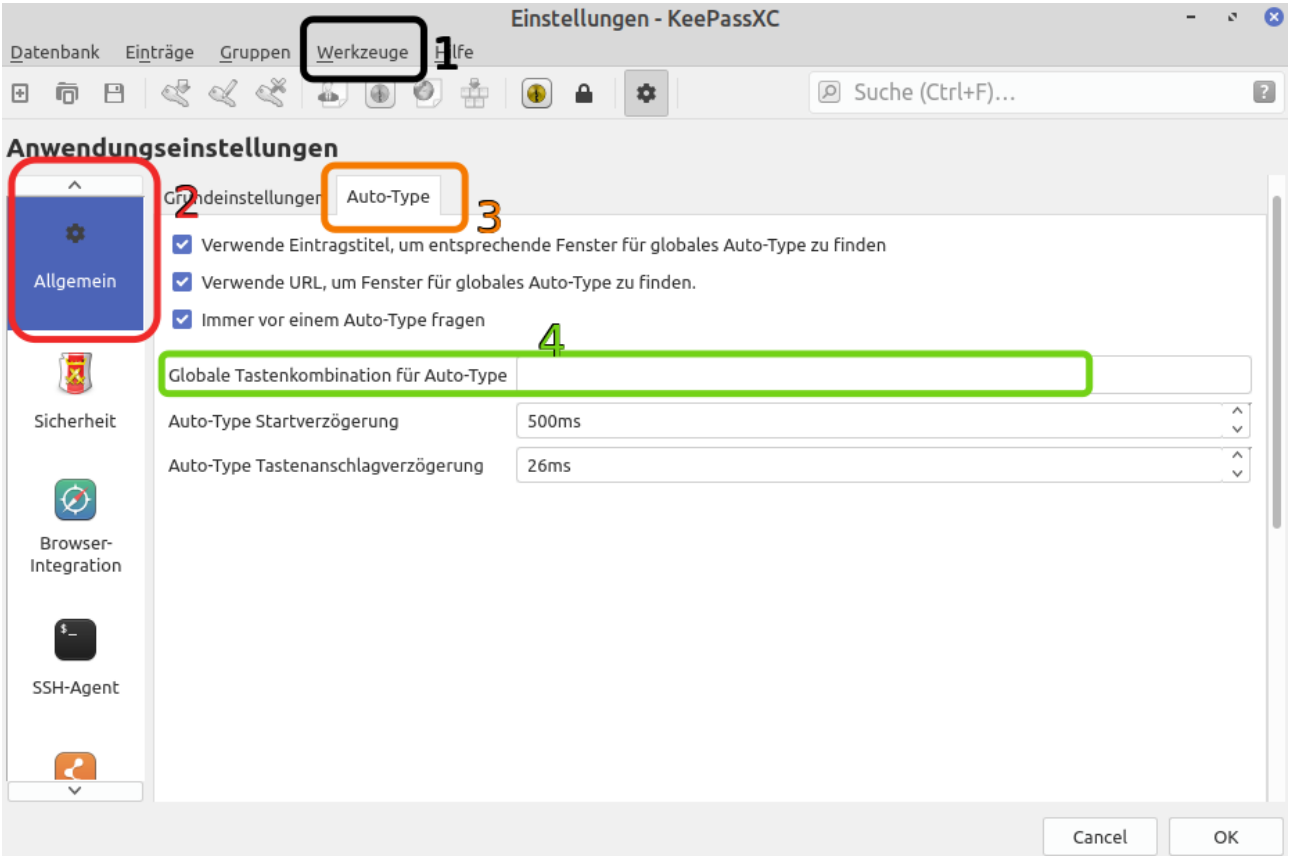
Deshalb sollte nach Möglichkeit **immer die Auto-Type-Funktion** genutzt werden (Strg+Shift+V). Dazu wird einfach der entsprechende Eintrag mit der linken Maustaste ausgewählt. Anschließend wird z.B. im Browser auf das Anmeldefenster, in dem man sich anmelden möchte, geklickt, um die Auto-Type-Funktion zu nutzen. (Hinweis: Sie lässt sich auch mit einem Rechtsklick auf den entsprechenden Eintrag im dann aufklappenden Menübaum auswählen).

Folgende Voraussetzungen müssen vorliegen, damit Auto-Type funktioniert:

- Die Datenbank muss entsperrt sein.
- Es müssen Benutzername und Passwort hinterlegt sein.
- Titel des Login-Fensters auf der Website und der Titel des Passworteintrags in der Datenbank sollten ähnlich sein, damit KeePassXC den entsprechenden Eintrag finden kann.

Die Auto-Type-Funktion kann unter den folgenden Einstellungen einer anderen Tastenkombination zugewiesen werden:

- ***Menüleiste Werkzeuge [1] → Einstellungen → Allgemein [2] → Auto-Type [im Reiter neben Grundeinstellungen – 3] → Globale Tastenkombination für Auto-Type[4]***



Schritt 6: Sicheres Masterpasswort finden

Für ein sicheres Passwort ist die zufällige Auswahl entscheidend wichtig. Doch niemand ist in der Lage, sich eine wirklich zufällige Zeichenfolge auszudenken.

Deshalb bietet es sich an, mit einer Würfelliste eine Passphrase zu würfeln. Hierzu wird ein sechs-seitiger Würfel und eine Wortliste benötigt. Mithilfe der Wortliste können die gewürfelten Zahlen in Wörter „übersetzt“ werden. Eine solche Liste für verschiedene Sprachen kann z.B. hier heruntergeladen werden: https://theworld.com/~reinhold/diceware.html[1].

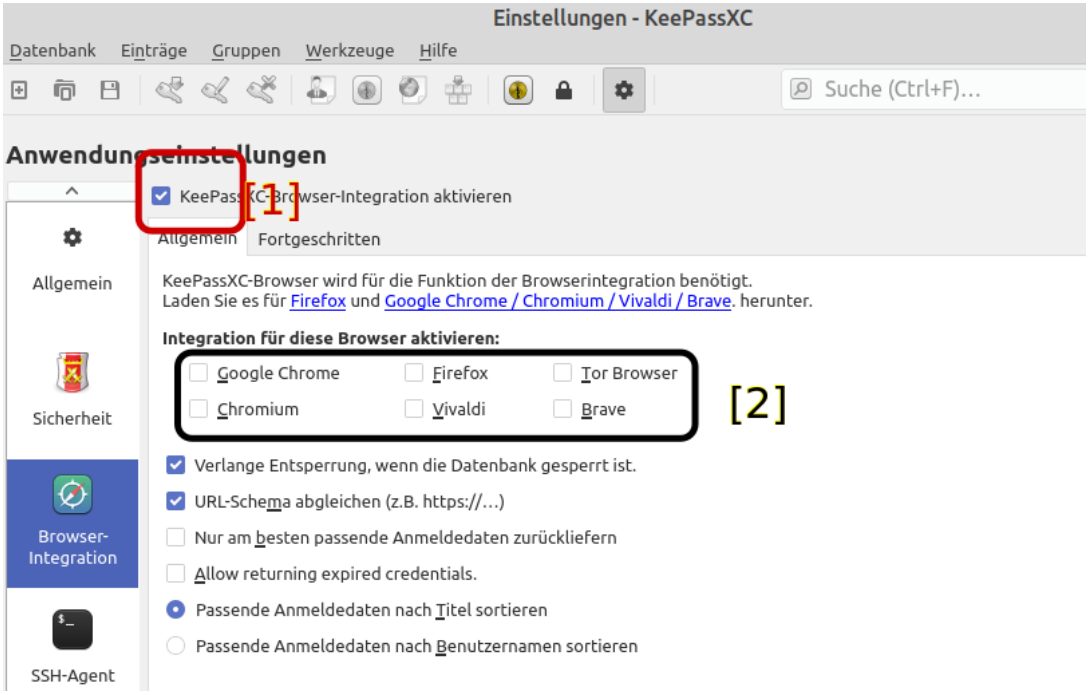
Funktionsweise: in jeder Spalte steht links eine fünfstellige Zahl und rechts daneben ein Wort. Mit dem Würfel wird nun für jedes Wort fünf Mal gewürfelt. Die gewürfelten Zahlen werden auf einem Blatt Papier notiert. Nehmen wir an, es wurde die Zahl 12546 gewürfelt. Verwendet man die oben erwähnte Liste in deutsch, so ist das dazugehörige Wort *ahorn*. Das ist das erste Wort. Diesen Vorgang wird beliebig oft, mindestens aber sechs mal, wiederholt. So werden insgesamt insgesamt mindestens (6 * 5 =) 30 Würfe benötigt. Mit dieser Anzahl an Würfen wird ein hohes Maß an Zufälligkeit (Entropie) erzeugt. (Hinweis: 30 Würfe mit einem 6-seitigen Würfel entsprechen rund 78 zufälligen Bits.)

Die gewürfelten Worte ergeben hintereinander geschrieben die sichere Passphrase, welche bspw. so aussieht: *ahornGansFernseherwindigPflanzerot*

Exkurs: KeepassXC im Browser

Für KeepassXC gibt es ebenfalls ein Add-on für den Browser. Damit soll die Benutzerfreundlichkeit erhöht werden.

Voraussetzung für die Verbindung zwischen dem Browser-Add-on und der Datenbank ist die Freischaltung der Funktion in den Einstellungen von KeePassXC.



1 Zuletzt aufgerufen am 06.07.2022

- Menüleiste ***Werkzeuge → Einstellungen → Browser-Integration***
- Durch Linksklick wird das Kästchen ***KeepassXC-Browser-Integration aktivieren*** **[1]** ausgewählt. Dann ebenfalls mit Linksklick den **verwendeten Browser auswählen [2]**.

Außerdem wird das Add-on für den jeweils verwendeten Browser benötigt. Für Firefox findet man es in den Einstellungen unter dem Reiter *Add-ons* und dort unter dem Namen *KeePassXC-Browser.*

Nach dem beides geschehen ist, muss eine **Verbindung zwischen der Datenbank und dem Browser-Add-on hergestellt** werden. Hierzu wird in den Einstellungen des Add-ons über den Punkt *Verbundene Datenbanken [1]* über die Schaltfläche *Verbinden* [2] eine Datenbank hinzugefügt. Anschließend muss man einen Namen für die verbundene Datenbank festlegen. Der Zugriff zur Datenbank muss anschließend noch erlaubt werden [3].

KeePassXC wird dann anhand der hinterlegten Titel nach entsprechenden Einträgen in der Datenbank suchen. Sofern eine Übereinstimmung zwischen Login-Website und Datenbankeintrag gefunden wurde, fragt KeePassXC, ob das Add-on darauf zugreifen darf.

Zum **Umgang mit dem Add-on noch einige Hinweise**. Browser sind oftmals von Sicherheitslücken betroffen. Deshalb birgt dieser Ansatz gegenüber dem Auto-Type-Verfahren eine **erhöhte Angriffsfläche**. Deshalb gilt, den Browser mit Updates aktuell zu halten.

Link zum Vertiefen

Weiterführende Informationen gibt es im Benutzerhandbuch zu KeePassXC (auf Englisch): https://keepassxc.org/docs/KeePassXC_UserGuide.html