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 Hauptpasswort.

Schritt 1: Software installieren

KeePassXC kann unter https://keepassxc.org/download/ heruntergeladen werden.

Schritt 2: Sprache ändern

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

- Menüleiste ***Tools*** (Werkzeuge) → ***Settings*** (Einstellungen) → ***General*** (Allgemein) → ***User Interface*** (Benutzeroberfläche) → ***Language*** (Sprache)

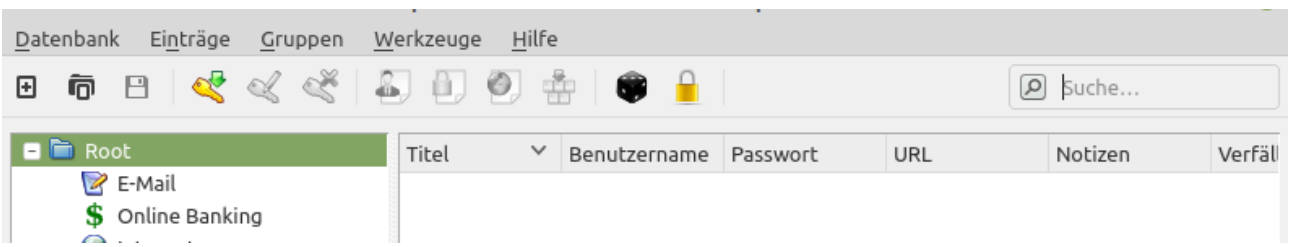
Schritt 3: Neue Passwort-Datenbank erstellen

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

Bei der **Passwort-Datenbank** handelt es sich um eine **wichtige Datei**. Sie trägt die Endung **.kdbx**. Die Passwörter werden ebenfalls verschlüsselt gespeichert, weshalb sie nur schwer rekonstruierbar sind. Deshalb ist es von **entscheidender Bedeutung**, dass das **Hauptpasswort sicher und gut merkbar** ist – **hiervon hängt die Sicherheit aller weiteren Passwörter ab** (→ dazu unten mehr). Aufgrund der Wichtigkeit der Datei, sollten regelmäßig Datensicherungen (sog. Backups) gemacht werden.

Schritt 4: Passworteinträge erstellen

Nun können im linken Bereich 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 in der Menüleiste erstellt. Alternativ ist auch ein Rechtsklick im rechten Bereich des Programms möglich. Die Datenbank bzw. Die Änderungen an Einträgen werden standardmäßig automatisch gespeichert.



Schritt 5: Passwörter verwenden

Ein in der Übersicht markiertes Passwort kann mittels „Kopieren“ (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). **Dieses ist kein sicherer Ort, da bösartige Software die Zwischenablage auslesen und dessen Inhalt an Dritte übermitteln könnte.**

Deshalb sollte nach Möglichkeit **immer die Auto-Type-Funktion** genutzt werden (Strg+Umschalt+V). Dazu wählt man einfach den entsprechenden Eintrag mit der linken Maustaste aus. 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).

Exkurs: Sicheres Hauptpasswort finden

Hierbei ist der Zufall entscheidend. Denn kein Mensch ist in der Lage, sich eine zufällige Zeichenfolge auszudenken.

Deshalb bietet es sich an, mithilfe einer Würfelliste, eine Passphrase zu würfeln. Ihr braucht dazu neben einem 6-seitigen Würfel noch eine Wortliste, mit deren Hilfe sich die Passphrase würfeln lässt. Eine solche findet ihr für verschiedene Sprachen z.B. unter: https://theworld.com/~reinhold/diceware.html#languages[1].

Funktionsweise: in jeder Spalte steht links eine fünfstellige Zahl und rechts daneben ein Wort. Jetzt nehmt ihr einen klassischen sechs-seitigen Spielwürfel. Für das erste Wort würfelt ihr fünf Mal. Die Zahlen notiert ihr euch auf einem Blatt. Nehmen wir an, es wurde die Zahl 12546 gewürfelt. Das dazugehörige Wort ist ahorn. Das ist euer erstes Wort. Diesen Vorgang wiederholt ihr beliebig oft, mindestens aber 6 Mal. So würfelt ihr insgesamt mindestens $6 \cdot 5 = 30$ Mal. Dadurch erzeugt ihr ein hohes Maß an Zufälligkeit (Entropie).

Die gewürfelten Worte ergeben hintereinander geschrieben eure sichere Passphrase.

1 Zuletzt aufgerufen am: 20.11.2020