**Einleitung: Authentifizierung und die Rolle von Passwortmanagern**

Die Authentifizierung ist ein zentraler Bestandteil der digitalen Sicherheit. Besonders wichtig ist die sichere Verwaltung von Passwörtern, da Wiederverwendung oder schwache Passwörter große Risiken darstellen. Passwortmanager ermöglichen die sichere Speicherung von Passwörtern in einer verschlüsselten Datenbank und bieten oft zusätzliche Funktionen wie die Unterstützung von Mehrfaktor-Authentifizierung (MFA). Diese verbessert die Sicherheit durch die Kombination von Wissen (z. B. Master-Passwort) und Besitz (z. B. Schlüsseldateien oder Hardware-Tokens).

**Diskussion: Kriterien für die Wahl eines Passwortmanagers**

Unsere Gruppe hat folgende Kriterien für die Wahl eines Passwortmanagers festgelegt:

1. **Sicherheit**:
   * Starke Verschlüsselung (z. B. AES-256 oder ChaCha20) für die Datenbank.
   * Unterstützung von Mehrfaktor-Authentifizierung (z. B. mit YubiKey).
2. **Benutzerfreundlichkeit**:
   * Intuitive Bedienung, auch für technisch weniger versierte Nutzer.
3. **Plattformübergreifende Verfügbarkeit**:
   * Der Passwortmanager sollte auf verschiedenen Geräten und Betriebssystemen (Windows, macOS, Linux, Android, iOS) nutzbar sein.

**Vergleich: Unsere Kriterien vs. Empfehlungen des Datenschutzbeauftragten**

Nach der Lektüre des Merkblatts des Datenschutzbeauftragten des Kantons Zürich haben wir festgestellt, dass wir wichtige Aspekte übersehen hatten:

* **Open Source**: Ein öffentlich einsehbarer Quellcode erhöht Transparenz und Sicherheit.
* **Speicherort der Daten**: Die Möglichkeit zur lokalen Speicherung der Passwortdatenbank wird bevorzugt, um die Abhängigkeit von Cloud-Diensten zu minimieren.
* **Zusätzliche Sicherheitsfunktionen**: Unterstützung von Schlüsseldateien oder Zwei-Faktor-Authentifizierung bietet zusätzlichen Schutz.

Neue Erkenntnisse aus dem Merkblatt: Neben unseren initialen Kriterien ist auch die **Transparenz (Open Source)** sowie der **kontrollierbare Speicherort** der Datenbank entscheidend.

**Vergleich und Auswahl eines Passwortmanagers**

**Anforderungen:**

1. **Verschlüsselung**: Muss mindestens AES-256 oder ChaCha20 unterstützen.
2. **Open Source**: Quellcode muss öffentlich einsehbar sein.
3. **Plattformübergreifend**: Verfügbarkeit auf PC, Smartphone und Tablet.
4. **Zusätzliche Sicherheitsfunktionen**: Unterstützung von Mehrfaktor-Authentifizierung (z. B. YubiKey).

**Vergleich:**

| **Passwortmanager** | **Verschlüsselung** | **Open Source** | **Plattformübergreifend** | **MFA-Unterstützung** |
| --- | --- | --- | --- | --- |
| **KeePassXC** | AES-256, ChaCha20 | ✓ Ja | ✓ Ja | ✓ Ja (z. B. YubiKey) |
| **LastPass** | AES-256 | ✗ Nein | ✓ Ja | ✓ Ja |
| **Bitwarden** | AES-256 | ✓ Ja | ✓ Ja | ✓ Ja |

**Begründete Wahl:**

Wir entscheiden uns für **KeePassXC**, da es alle unsere Anforderungen erfüllt: starke Verschlüsselung, Open Source, plattformübergreifende Verfügbarkeit und Unterstützung von Mehrfaktor-Authentifizierung. Besonders die lokale Speicherung der Datenbank erhöht die Kontrolle über die eigenen Daten.

**Einrichtung und Sicherheitsüberlegungen**

**Einrichtung:**

* **KeePassXC** wird auf PC und Smartphone installiert.
* Die Passwortdatenbank wird lokal gespeichert und regelmäßig gesichert.
* MFA wird mit einem YubiKey als zweitem Faktor eingerichtet.

**Was tun, wenn...**

1. **...das Master-Passwort vergessen wird?**
   * Backup-Codes werden sicher offline aufbewahrt.
2. **...die Passwortdatenbank beschädigt wird?**
   * Regelmäßige Backups auf einem verschlüsselten USB-Stick oder einer lokalen Festplatte.
3. **...kein Zugriff auf den Cloud-Dienst besteht (falls genutzt)?**
   * Die Passwortdatenbank wird lokal gespeichert, um keine Abhängigkeit von der Cloud zu haben.

**Fazit**

Passwortmanager wie KeePassXC bieten eine sichere, benutzerfreundliche Lösung für die Verwaltung von Passwörtern. Die Kombination mit Mehrfaktor-Authentifizierung und einer lokal gespeicherten, verschlüsselten Datenbank bietet ein hohes Maß an Sicherheit und Kontrolle.