Merkblatt 08

Empfehlungen Passwortmanager

1. Einleitung

Der Zugang zu IT-Diensten der Zentralen Informatik erfolgt in der Regel über Azure Active Directory oder SWITCH edu-ID. Nutzende müssen sich dadurch nur diese zwei unterschiedliche Passwörter merken. Trotzdem werden meist noch viele weitere Anwendungen verwendet, für die aus Sicherheitsgründen für jedes Konto ein anderes und starkes Passwort erforderlich ist. In der Praxis führt diese zu unzähligen Passwörtern, die sich kaum noch jemand im Kopf speichern kann. Mit einem Passwortmanager lässt sich dieses Problem in den Griff bekommen. Er erleichtert die Erstellung und Nutzung sicherer Passwörter, weil man sich nur das Master-Passwort für den Passwortmanager merken muss.

Die Zentrale Informatik hat in Zusammenarbeit mit der Abteilung Recht und Datenschutz eine Auswahl verbreiterter Passwortmanager auf Datenschutz, IT-Sicherheit, Funktionalität und Benutzerfreundlichkeit geprüft, mit dem Ziel eine Empfehlung abgeben zu können. Insgesamt wurden 25 Kriterien bewertet.

2. Empfehlungen

Insgesamt spricht die Zentrale Informatik für drei Lösungen eine Empfehlung aus.

Kostenlose Lösung: KeePass2 - https://keepass.info/
KeePass2 ist ein kostenloser Open Source Passwort Manager, der für eine sicherere Speicherung von Passwörtern empfohlen werden kann. Die Daten werden dabei lokal auf einem Gerät gespeichert. Eine Synchronisation zwischen mehreren Geräten und eine Browser-Integration kann über Plug-Ins und Drittanbieter möglich gemacht werden. Diese sind jedoch auf Datenschutz und Datensicherheit zu prüfen. Die Benutzerfreundlichkeit beurteilen wir als durchschnittlich. KeePass2 steht auf dem Digitalen Arbeitsplatz der Zentralen Informatik allen Nutzenden als optionale Software zur Verfügung.

Cloud-Lösung: 1Password - https://1password.com
1Password ist eine Cloudlösung. Damit ist vor dem Einsatz eine Risikoabwägung notwendig. Die Einführung stellt eine Datenbearbeitung im Auftrag dar, womit entsprechenden Voraussetzungen, wie unter anderem den Abschluss eines entsprechenden Vertrags unter Beizug der Datenschutz AGB, eingehalten werden müssen (weitere Informationen siehe Link). Die nutzenden Organisationseinheit oder die zuständigen IT-Verantwortlichen sind aufgefordert, geeignete organisatorische und/oder technische Massnahmen einzuführen, um den Alltagsbetrieb sicherzustellen (insbesondere bei Verlust des Master-Passworts). Der Anbieter bietet insgesamt gute IT-Sicherheitsfunktionen und akzeptiert die Allgemeinen Geschäftsbedingungen der UZH, respektive die SIK AGB und UZH AGB DS Auslagerung IT. Zudem zeichnet sich das Produkt durch vielfällige Integrationsmöglichkeiten und eine sehr gute Benutzerfreundlichkeit aus.

On-Prem Serverlösung: Passwork https://passwork.de
Die Software Passwork als «selbstgehostete Version» - also installiert auf eigenen Servern - eignet sich für alle Arten von Passwörtern. Sie bedingt jedoch Infrastruktur und führt damit zu betrieblichem Aufwand bei der IT. Passwork bietet ebenfalls eine gute Benutzerfreundlichkeit und einen grossen Funktionsumfang.

3. Einsatz eines Passwortmanagers

Die Entscheidung ob und wenn ja welcher Passwortmanager eingesetzt werden soll, liegt bei der jeweiligen UZH-Organisationseinheit und den zuständigen IT-Verantwortlichen, genauso dass die Vorgaben zu Informationssicherheit, IT-Sicherheit und Datenschutz eingehalten werden. Finanzierung, Bestellung, Bereitstellung und Verwaltung erfolgt ebenfalls durch die IT-Verantwortlichen der jeweiligen Organisationeinheit.