

Workshop: Passwort-Manager im Multi-Device-Setup – Nutzung und Synchronisation einer zentralen Passwort-Datenbank

Passwörter sollten individuell und komplex sein. Niemand kann sich jedoch 100 verschiedene Passwörter merken. In der Praxis führt das dazu, dass für verschiedene Dienste identische, leicht zu knackende Passwörter verwendet werden. Abhilfe schafft ein Passwort-Manager, der automatisch generierte Passwörter in einer verschlüsselten Datenbank speichert. So muss man sich nur noch ein einziges Passwort merken, das für die Passwort-Datenbank. Damit die Passwörter jederzeit zur Verfügung stehen, wenn sie gebraucht werden, muss die Datenbank online verfügbar und jederzeit von überall abrufbar sein.

Dieser Workshop soll zeigen, wie eine entsprechende Datenbank mittels KeePass erstellt wird, wie die zukünftige Registrierung bei Diensten damit abläuft und wie diese Datenbank zwischen allen Geräten des Nutzers synchron gehalten werden kann.

Da wir keine Cloud-Dienste von Drittanbietern nutzen wollen, setzen wir eine Owncloud auf einem Raspberry Pi auf, der beim Nutzer zu Hause steht. Dazu sind keine oder kaum Linux-Kenntnisse erforderlich. Der Workshop sollte also auch für technisch Unbedarfte nachvollziehbar und reproduzierbar sein.

Folgende Punkte stehen für diesen Workshop auf dem Programm:

- Installation von ArkOS <https://arkos.io/> auf einem Raspberry Pi
- Einrichtung von Owncloud
- Einrichtung von KeePass inklusive Erstellung einer Passwort-Datenbank
- Einrichtung des DB-Backups mit <http://keepass.info/plugins.html#dbbackup>
- Konfiguration des Routers zum Fernzugriff auf die Datenbank
- Einrichten der Synchronisierung mit der Owncloud
- Einrichtung auf mobilen Geräten

Nach Absolvieren des Workshops verfügt jeder Teilnehmer über eine eigene Datenbank zur sicheren Verwahrung seiner Passwörter, und das ganze nicht bei einem mehr oder weniger vertrauenswürdigen Internetdienst, sondern auf eigener Hardware, die bequem zu Hause an den Internet-Router angeschlossen werden kann. Ebenso verfügen die Teilnehmer nun über die Möglichkeit, von mehreren, wenn nicht allen internetfähigen Geräten auf diese Datenbank zuzugreifen und sie für passwortbasierte Logins zu nutzen. Die Sicherheit der Teilnehmer im Internet erhöht sich damit deutlich, da keine schwachen, leicht zu merkenden oder auch ähnlichen Passwörter für verschiedene

Dienste benutzt werden. Man muss sich nur noch ein komplexes Passwort für die Datenbank merken während für die genutzten Internetdienste können wirklich sichere, auf Zufall basierende Passwörter genutzt werden, die sich nicht erraten lassen.

Der Workshop beinhaltet auch es eine kurze Einführung in die 2-Faktor-Authentifizierung.