Frank Waldschmidt-Dietz, Universitätsbibliothek Gießen (2020)

KeePass icon von Nardog, GNU General Public License, via Wikimedia Commons.

Passwortsicherheit und der Passwortmanager KeePass 2

„Das größte Problem für die Sicherheit persönlicher Daten sind nicht gewiefte Hacker, sondern die schlechten Passwörter überforderter Anwender.“
(dpa, jnm, t-online.de 2020)

Inhalt

1 Einleitung

1.1 Warum und wozu benötigt man einen Passwortmanager (PM) wie KeePass 2?

Wir sind und bleiben bequem – das ist normal. Unsere Passwörter sind daher in der Regel…

- … gering an der Zahl,
- leicht zu merken,
- für mehrere Dienste in Verwendung,
- „irgendwo“ gespeichert oder schriftlich abgelegt, …

… kurzum: **unsicher**!

Professionelle Hacking-Tools sind gleichzeitig leicht verfügbar, so dass auch Laien leichtes Spiel hätten, würden wir in ihr Visier geraten – von Profis mal ganz abgesehen.

Wenn Zugangsdaten abhandenkommen, wird das meist aber nicht einmal an uns selbst oder unserem ausgespähten Computer liegen. Es genügt völlig, wenn ein Dienst gehackt wird, bei dem wir registriert waren. Mir ist das schon bei mittlerweile einigen Diensten passiert – auch prominente, wie z.B. Adobe und dropbox waren bereits Opfer von Hackern und Nutzerdaten wurden gestohlen. Bislang ohne schlimme Folgen bei mir, da ich meine Passwörter seit vielen Jahren mit KeePass erzeuge und verwalte.

Ein Passwortmanager (PM) hilft also bei der Lösung o.g. Probleme. Ein PM ist eine Datenbank mit Zusatzfunktionen und enthält die Zugangsdaten zu unseren verschiedenen (Internet-) Diensten. Außerdem hilft er beim Erstellen und Verwalten komplexer und guter Passwörter. Merken muss man sich nur noch das (besonders sichere) Masterpasswort, welches die Datenbank absichert. Eine geräteübergreifende Nutzung ist meist möglich. Für die gemeinsam mit anderen Personen zu nutzenden Passwörtern kann ggf. eine zusätzliche gemeinsame Datenbank genutzt werden.

Unter Einsatz eines PM können und sollten unsere Passwörter

- Unikate sein,
- komplex sein (und daher meist nicht mehr zu merken),
- nur für *einen* einzigen Dienst im Einsatz sein.

KeePass 2 (https://keepass.info/) ist ein kostenloser PM, OpenSource, sehr weit verbreitet und gut bewertet. Es gibt eine Reihe weiterer PM, auch in Browsern sind i.d.R. ähnliche Lösungen integriert (Stiftung Warentest 2020).

Die Videos von ▸ Mobilsicher und ▸ CYBERDYNE fassen die Gründe für den Einsatz eines PM sehr gut zusammen.

1.2 Checklisten für Ihre Achtsamkeit

Ein Passwortmanager ist zwar ein hervorragendes Werkzeug für die Sicherheit im Netz, kann aber nicht ***Ihre*** Achtsamkeit ersetzen. Sie müssen grundlegende Sicherheitsaspekte beachten, damit Sie sich nicht in falscher Sicherheit wähnen. Das Herzstück des vorliegenden Dokumentes ist daher der Abschnitt „**Checklisten“** in Kapitel 3. Dort werden verschiedene Sicherheitsaspekte checklistenartig dargestellt.

2 Die Bedienung von KeePass 2

Die Bedienung von KeePass kann gut z.B. anhand der Videos von ▸ Simon oder ▸ PC-Welt nachvollzogen werden.

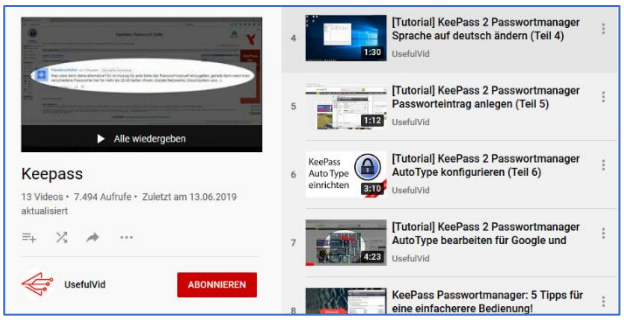
In der Navigation links auf der Homepage von KeePass (https://keepass.info/) findet sich eine ausführliche Dokumentation inklusive einer Hilfe, einer FAQ und einem Forum.

Folgendes Wissen im Umgang mit KeePass sollten Sie sich mit diesen Quellen aneignen:

1. Installation (im Unternehmen ggf. IT kontaktieren)
2. Programmoberfläche
3. Anlegen einer Datenbank
4. Anlegen und Speichern von Einträgen
5. Übertragung der Zugangsdaten zu den Diensten
6. Sicherheitsfeatures

Screenshot YouTube, nicht unter freier Lizenz

In der YouTube-Playlist von ▸ UsefulVid werden einige nützliche Zusatzfunktionen gezeigt, beispielsweise wie das Sprachpaket „Deutsch“ installiert wird, oder wie Auto-Type für Seiten angepasst werden kann, bei denen Benutzername und Passwort auf unterschiedlichen Seiten eingegeben werden müssen.



Screenshot YouTube, nicht unter freier Lizenz

3 Checklisten

3.1 Passwortsicherheit

- ☐ Jeder Dienst bekommt sein eigenes Passwort
- ☐ Die Passwörter sind komplex (z.B. Länge, Sonderzeichen)
- ☐ Passwörter bestehen aus Zufallsmustern
- ☐ Das Masterpasswort
  - ist besonders komplex bzw. lang
  - als *einziges* merkbar
- ☐ Verwendung der Zwei-Faktoren-Authentifizierung (2FA)

3.2 Gefahrenquellen

- ☐ Hacks von Diensten, bei denen man registriert ist
- ☐ Brute-force-Angriffe
- ☐ Phishing
- ☐ System-Hack (ungute Folgen sind z.B. Keylogger oder Mailabgriff)
- ☐ Kolleg_innen
- ☐ Fremde Rechner

3.3 Generelle Sicherheit

(Quelle: Stiftung Warentest 2020)

- ☐ Geräte sichern/ sperren
- ☐ E-Mail-Konto schützen
- ☐ Hack-Check (https://haveibeenpwned.com/, https://sec.hpi.de/ilc/)
- ☐ Vorsicht vor Phishing
- ☐ Achtung bei Browsern
- ☐ Alte Konten löschen
- ☐ Ändern ist out, Komplexität ist besser

3.4 Empfehlenswerte KeePass-Optionen/Funktionen

- ☐ Emergency-Sheet ausdrucken
- ☐ Gute Passwörter generieren lassen
- ☐ Auto-Type nutzen
- ☐ Auto-Type-Option: “two-channel obfuscation” hilft gegen Keylogger
- ☐ Auto-Type-Option: „at two step“ hilft bei Eingabe von Benutzername & Passwort auf unterschiedlichen Seiten
- ☐ Automatischer Workspace-lock, z.B. nach 2 Minuten
- ☐ Schlüsseldatei verwenden als zweiten Faktor
- ☐ Duplikate ermitteln

3.5 Sonstiges

- ☐ Regelmäßige Datenbank-Backups
- ☐ Gedruckte Passwortliste an *sicherem* Ort verwahren
- ☐ Masterpasswort an Vertrauensperson für den Notfall (im Umschlag) weitergeben

4 Nachweise

Literatur

Stiftung Warentest (2020): Einer für alle. Passwortmanager. In: *Test* (2), S. 28–35.

Webseiten

dpa, jnm, t-online.de (2020): Stiftung Warentest: Einen der besten Passwortmanager gibt es kostenlos. Online verfügbar unter https://www.t-online.de/digital/software/id_87231976/stiftung-warentest-einen-der-besten-passwortmanager-gibt-es-kostenlos.html.

Reichl, Dominik (2020): KeePass-Homepage. Online verfügbar unter https://keepass.info/index.html.

Videos

CYBERDYNE (2017): Unverzichtbare Tools: Wieso wir alle Passwortmanager nutzen sollten. YouTube. Online verfügbar unter https://www.youtube.com/watch?v=UHMpZyByRKw.

Mobilsicher (2020): Was können Passwortmanager? Empfehlung KeePass | feat. Alex von Privacy Tutor. YouTube. Online verfügbar unter https://www.youtube.com/watch?v=pw71exFa8Ow.

PC-Welt (2012): Passwörter verwalten mit KeePass 2 - so geht‘s. YouTube. Online verfügbar unter https://www.youtube.com/watch?v=tX-Izo7o4a4.

Simon (2019): Deine Passwörter sicher verwalten | KeePass 2 (Tutorial). YouTube. Online verfügbar unter https://www.youtube.com/watch?v=6JlboO-kiEU.

UsefulVid (2019): Playlist „Keepass“. YouTube. Online verfügbar unter https://www.youtube.com/playlist?list=PLYxp-Xxp1C7zZCMVjie0tHxpSq-puSfdw.