DIDAY: Passwort-Manager

Ihr kennt es alle: ihr meldet euch in einer App oder auf einer Website neu an, und ihr braucht ein gutes Passwort. Aber wo bekommt man das her, und noch viel wichtiger, wie merkt man sich das? Über die Zeit kommen schnell zig wenn nicht hunderte solche Passwörter zusammen.

Beim DIDAY im Juli zeigen wir euch bei uns im CCCHH, welche Optionen es gibt, und welche Vor- und Nachteile sich damit verbinden: unterschiedliche Passwort-Manager rein lokal auf dem eignenen Rechner, mit Synchronisierung über NextCloud, oder mit Cloud-Dienst. Und wir haben auch eine ganz einfach Papier-Variante, die trotzdem sicher ist!

Warum Passwort-Manager?

- Ein Passwort für alles ist nicht gut
  - Wenn das Passwort jemand bekannt wird, muss man sein Passwort bei allen Apps und Websites ändern
  - Am besten also ein individuelles Passwort für jeden Dienst
- Man kann sich so viele Passwörter nicht merken
- Die besten Passwörter kann man sich überhaupt nicht merken
- Passwort-Manager:
  - helfen, gute Passwörter zu verwenden (bei der Registrierung)
  - Können Benutzername und Passwort automatisch ausfüllen
  - können Passwörter auf mehreren Geräten zur Verfügung stellen
  - Können auch weitergehende Daten sicher speichern

Mein Telefon/Browser macht Passwörter

- Mein Telefon/mein Browser schlagen bei der Registrierung gute Passwörter vor, und füllen sie automatisch aus. Reicht das nicht?
- Für die meisten Belange OK:
  - Apple iPhone/iPad/Mac
  - Google Pixel mit Chrome (Telefon/Tablet)
  - Microsoft Edge (auf Windows und Mac)
- Aber:
  - Bei Geräteverlust muss man trotzdem noch Zugriff auf den Cloud-Account haben
  - Ich arbeite mit Geräten unterschiedlicher Hersteller
  - Funktioniert nicht mit allen Apps/Websites
  - Abhängigkeit von einem (großen) Hersteller
  - Gute Backups vom Handy sind sehr wichtig

Passwort-Manager: Funktionen

- Ein Haupt-Passwort für den Passwort-Manager: das einzige Passwort, was man sich noch merken muss
- Synchronisation aller Passwörter über Cloud (verschlüsselt)
  - Alle Einträge stehen auf allen Geräten zur Verfügung
- Direkte Integration ins Betriebssystem und Browser
  - Ausfüllen von Anmeldemasken mit einem Klick/Tap
  - Bei Registrierung automatisch gutes Passwort einfüllen und speichern
  - Zwei-Faktor-Daten (OTP)
- Weitere sensitive Daten können gespeichert werden
  - Kredit- und andere Karten
  - Ausweise
- Passkey über Geräte hinweg

Passkeys

- Verschlüsselte Verbindung zwischen Website, Account und Endgerät
- Der Login funktioniert nur auf der festgelegten Website (Phisher können die Daten nicht abgreifen)
- Je nach Passwortmanager können Passkeys zwischen Geräten synchronisiert werden
- Bequem, weil der Browser das schnell und einfach ausfüllt und man schnell angemeldet ist
- Aber: Username und Passwort funktionieren immer noch, und wenn man das auf der falschen Seite eintippt, ist man trotzdem verloren
- Nicht alle Webseiten unterstützen Passkeys (oder nicht vollständig)

Zwei-Faktor-Authentifizierung

- Grundidee: Zwei unterschiedliche (geheime) Dinge zur Anmeldung notwendig
- Mögliche Faktoren:
  - Passwort
  - One-Time-Passwort (bekannt durch Google oder Microsoft Authenticator)
  - Passkey
  - Hardware-Token
  - Biometrische Merkmale (Fingerabdruck, Gesicht, …)
- Passwort-Manager mit OTP-Unterstützung
- Hardware-Token: Super sicher, aber komplizierter in der Einrichtung/Anmeldung und Anwendung

Andere Verfahren

- Login per Email/SMS: man gibt seine Email-Adresse oder Telefonnummer ein und bekommt eine Mail/SMS mit einem Code
  - Bei Verlust der Email/Telefonnummer kann der Account verloren sein
  - Wenn dritte Kontrolle über Email/Telefonnummer haben, können sie den Code abfangen
- Login per Google/Apple/Facebook: die Website leitet für die Anmeldung an einen der großen Dienste weiter
  - Sehr bequem, aber abhängig vom Dienst
  - Daten werden an den Dienst weitergegeben

Welcher Passwort-Manager?

- Einfache Möglichkeit des Backups
- Möglichst viele unterstützte Plattformen
- Synchronisation über Geräte hinweg
- OTP-Unterstützung
- Gute Import- und Export-Möglichkeiten
- Unabhängig von großen Anbietern (Open Source)
- Unabhängig von großen Clouds (Sync über Nextcloud etc.)
- Umgang des Herstellers mit Sicherheitslücken
- Gute Integration in das Betriebssystem/Handy

bitwarden

- Cloud-Service
  - Kostenloses Angebot mit Einschränkungen
  - Für Privatkunden zwischen ca 2€ und 6€ pro Nutzer
- Clients Open Source
- Open-Source-Implementation VaultWarden für das selber Hosten des Servers
- Gute Integration in alle üblichen Betriebssysteme und Browser
- Unterstützt Passkeys, OTP und viele Datenformate
- Kleines Fragezeichen, ob es Open Source bleiben wird
- Amerikanisches Unternehmen
- Im- und Export
- Kein automatisches Backup

1Password

- Cloud-Service
  - Für Privatkunden zwischen ca. 3€ und 6€ pro Nutzer
- Closed Source
- Gute Integration in alle üblichen Betriebssysteme und Browser
- Unterstützt Passkeys, OTP und viele Datenformate
- Amerikanisches Unternehmen
- Im- und Export mit vielen Formaten
- Kein automatisches Backup

Keepass/KeepassXC

- Offenes Dateiformat und Open- und Closed-Source Clients
- Teilweise Browser-Integration (je nach Client)
- Unterstützung von Passkeys, OTP je nach Client
- Software-Lizenzen/Kosten:
  - KeypassXC: GPL
  - Keepassium: kostenlos, erweiterte Features ab €20 pro Jahr
  - Strongbox: kostenlos, erweiterte Features ab €25 pro Jahr
- Im- und Export mit vielen Formaten je nach Client
- Passwort-Datenbank liegt auf dem Gerät
  - Einfaches Backup per System
  - Synchronisation per NextCloud, Synology, etc.
- Sync direkt aus dem Client heraus (z. B. Strongbox)

LastPass

- Kommerzielle Software
- In der Vergangenheit sehr schwere Sicherheitslücken und schlechte Reaktion des Herstellers
- Bis auf weiteres klare Empfehlung dagegen

Apple Schlüsselbund

- Tiefe Integration in das Betriebssystem
- Synchronisation auf alle Apple-Geräte mit iCloud
- OTP und Passkeys
- Backups über TimeMachine und iCloud
- Keine Unterstützung außerhalb der Apple-Welt (eingeschränkte Funktion in Windows)

Papier-Lösung

1. Teil des Passworts merken

- Für jeden Account gleich
- Ohne persönlichen Bezug
- Mindestens acht Zeichen lang
- Besteht bspw. aus zwei ausgedachten, aneinander gereihten Wörtern (tisch-himmel)

+

2. Teil des Passworts in Liste eintragen

- Für jeden Account anders
- Entweder kurz und komplex oder besonders lang
- Besteht bspw. aus willkürlich aneinander gereihten Zeichen oder aus vier Wörtern, die durch Sonderzeichen getrennt sind (Berg_spät_hüpfen_Kühlschrank)

=

Sichere Passwörter für jeden Account

(tisch-himmelBerg_ spät_hüpfen_Kühlschrank)

Account	Nutzername/ E-Mail-Adresse	2. Teil des Passworts
1. Musteraccount	maxine@musterfrau.de	Berg_spät_hüpfen_Kühlschrank
2. Musteraccount	maxine@musterfrau.de	q7yPv8!x§B2

Quellen

- BSI-Leitfaden Passwörter merken