dsb

datenschutzbeauftragte
kanton zürich

Merkblatt

Passwortmanager

1 Einleitung

Für die sichere Verwendung von Onlinediensten ist für jedes Konto ein anderes und starkes Passwort erforderlich. In der Praxis führt diese Regel zu unzähligen Passwörtern, die man sich merken muss. Mit spezieller Software, sogenannten Passwortmanagern, lässt sich dieses Problem in den Griff bekommen. Sie erleichtern die Erstellung und Nutzung sicherer Passwörter, weil man sich nur noch wenige merken muss: diejenigen für die wirklich sensiblen Dienste sowie das Master-Passwort für den Passwortmanager.

Dieses Merkblatt enthält eine sicherheitstechnische Analyse sowie einen Vergleich der folgenden Passwortmanager und beschreibt, wie KeePass2, MiniKeePass und KeePass2Android installiert und konfiguriert werden können.

- 1Password
- Bitwarden
- KeePass2
- MiniKeePass
- KeePass2Android
- LastPass
- Schlüsselbundverwaltung / Keychain
- SecureSafe

2 Kriterien

Kriterien	Beschreibung
Betriebssystem	Beschreibt, auf welchen Betriebssystemen (Windows, MacOS, iOS, Linux oder Android) der Passwortmanager genutzt werden kann.
Quellcode verfügbar	Beschreibt, ob der Programmcode öffentlich verfügbar ist. Dies ist sicherheitsrelevant, da ein öffentlich verfügbarer Quellcode (Open Source) besser auf Schwachstellen überprüft werden kann.
Brute-Force-Schutz	Beschreibt, welche Schutzmassnahme gegen Brute-Force-Angriffe (Durchprobieren aller möglichen Passwörter) existiert.
Keylogger-Schutz	Beschreibt, welche Schutzmassnahme gegen Keylogger-Angriffe (Aufzeichnen der Tastatureingaben) existiert.
Schutz Zwischenablage	Beschreibt, wie die Zwischenablage gegen Auslesen geschützt ist.
Automatische Sperre	Beschreibt, ob die Passwortdatenbank nach einer gewissen Zeitspanne automatisch gesperrt wird.
Authentifizierung	Beschreibt die Möglichkeiten zur Authentifizierung gegenüber dem Passwortmanager.
Automatische Passwortgenerierung	Gibt an, ob sich sichere Passwörter automatisch generieren lassen.
Ablageort Datenbank	Beschreibt, wo die Passwortdatenbank gespeichert wird.
Verschlüsselung Datenbank	Beschreibt, mit welchem Algorithmus und welcher Schlüssellänge die Passwortdatenbank verschlüsselt wird.
Passwortwiederherstellung	Beschreibt, ob und wie das Master-Passwort wiederhergestellt werden kann.
Synchronisation	Beschreibt, ob sich die Passwörter über verschiedene Systeme synchronisieren lassen. Eine automatische Synchronisation erhöht die Benutzerfreundlichkeit, aber auch die Risiken.
Portability (Export)	Beschreibt, in welchem Format die Passwörter zur weiteren Verwendung exportiert werden können.

3 Analyse und Vergleich

Produkte / Kriterien	KeePass-Datenbanken			1Password	Bitwarden	LastPass	Schlüsselbund-verwaltung / Keychain	SecureSafe
	KeePass2	**MiniKeePass**	**KeePass2 Android**					
Windows	**x**				**x**	**x**		**x**
MacOS	**x**				**x**	**x**	**x**	**x**
Linux	**x**				**x**	Add-on		
Android			**x**		**x**	**x**		**x**
iOS		**x**			**x**	**x**	**x**	**x**
Brute-Force-Schutz	Schlüssel-transformation	Schlüssel-transformation	Schlüssel-transformation	PBKDF2	PBKDF2	PBKDF2	*Keine Informationen verfügbar*	PBKDF2
Keylogger-Schutz	TCATO / Secure Desktop (Master-Passwort)	Guter Schutz durch App-Rechte-management	Eigene Software-tastatur	*Keine Informationen verfügbar*	*Keine Informationen verfügbar*	Virtuelle Tastatur	*Keine Informationen verfügbar*	–
Schutz Zwischenablage	Automatische Löschung	Automatische Löschung	Eigene Software-tastatur	Automatische Löschung	*Keine Informationen verfügbar*	Automatische Löschung	*Keine Informationen verfügbar*	Automatische Löschung
Automatische Sperre	Ja	Ja	Ja, Quick-Unlock-Schlüssel	Ja	Konfigurierbar	Ja	Ja	Ja
Verschlüsselung Datenbank	AES256	AES256	AES256	AES256	AES256	AES256	AES256	AES256

Produkte / Kriterien	KeePass-Datenbanken			1Password	Bitwarden	LastPass	Schlüsselbund-verwaltung / Keychain	SecureSafe
	KeePass2	**MiniKeePass**	**KeePass2 Android**					
Authentifizierung	Passwort / Schlüs-seldatei / OTP (OATH/HOTP), Yubikey, Google Authenticator usw.	Passwort / Schlüsseldatei	Passwort / Schlüs-seldatei / OTP (OATH/HOTP) / Yubikey	Passwort	Benutzername / Passwort, Authy, Google Authentica-tor Kostenpflichtig: SMS, Yubiykey	Benutzername / Passwort, Yubikey, Google Authentica-tor, OTP, Finger-print usw.	Passwort / iCloud Zwei-Faktor	Benutzername / Passwort / mTan (kostenpflichtig)
Automatische Passwortgenerie-rung	Ja	Ja	Ja		Ja	Ja	Ja	Ja
Ablageort Datenbank	Lokal	Lokal	Lokal	Standard in der Cloud, lokal mög-lich[1]	Lokal[2] oder in der Cloud gespeichert	In der Cloud ge-speichert	Lokal oder in der iCloud	In der Cloud (CH) gespeichert
Synchronisation	Über Drittdienste (siehe Merkblatt Online-Speicherdienste)			Ja	Ja			
Passwort-wiederherstellung	–	–	–	Ja (Emergency Kit)	–	Passworthinweis, Back-up-Schlüssel und E-Mail	Nur bei iCloud Synchronisation	Wiederherstel-lungscode
Portability (Export)	CSV / HTML	CSV / HTML (über PC-Anwendung)	CSV / HTML	CSV	CSV	CSV		CSV

[1] Lokales Speichern über lokaler Ordner (Local Folder / Vault) möglich
[2] Lokales Abspeichern der Bitwarden-Passwortdatenbank vor allem für Expertinnen oder Experten

Produkt- und Herstellerinformationen								
Hersteller	Dominik Reichl (DE) http://www.dominik-reichl.de	Flush Software, LLC (USA) http://minikeepass.github.io	Philipp Crocoll (DE) http://philipp.crocoll.net/donate.php	AgileBits, Inc. (CA) https://www.1password.com	8bit Solutions LLC https://bitwarden.com	Marvasol Inc. (USA) https://www.lastpass.com	Apple Inc. (USA) https://www.apple.com	DSwiss AG (CH) https://www.securesafe.com
Quellcode verfügbar	Quellcode verfügbar	Quellcode verfügbar	Quellcode verfügbar	Quellcode nicht verfügbar	Quellcode verfügbar	Quellcode nicht verfügbar	Quellcode teilweise verfügbar	Quellcode nicht verfügbar
Preis	kostenlos	kostenlos	kostenlos	Ab $3 pro Monat	kostenlos / Premiumdienste ab $12 pro Jahr	Ab 3$ pro Monat (eingeschränkt: kostenlos)	kostenlos	Ab CHF 1.50 pro Monat (eingeschränkt kostenlos)
Bemerkungen	Sehr grosser Funktionsumfang				Benutzerfreundlich	Gute Dokumentation, sehr benutzerfreundlich		

	sehr sicher / sehr vertrauenswürdig		sicher / vertrauenswürdig		weniger sicher / weniger vertrauenswürdig

4 Tipp

KeePass2, KeePass2Android und MiniKeePass sind kostenlos verfügbare, sichere und ausgereifte Passwortmanager-Programme. 1Password, LastPass oder SecureSafe bieten umfangreichere Synchronisationsoptionen, sind jedoch kostenpflichtig. Zudem werden bei diesen Produkten die Schlüssel extern abgespeichert, wodurch die Sicherheit der Daten nicht komplett gewährleistet ist.

5 Restrisiken

Beim Einsatz eines Passwortmanagers besteht das Risiko darin, dass alle Passwörter an einem Ort gespeichert sind und durch einen Trojaner ausgelesen werden können. Um das Risiko eines Trojanerbefalls zu reduzieren, muss das Endgerät mit folgenden Massnahmen geschützt werden:

- Regelmässige Aktualisierung durchführen (Betriebssystem wie Windows, Programme wie Browser und Flash Player)
  - Weitere Informationen im Leitfaden Patch-Management des Bundesamts für Sicherheit in der Informationstechnik (BSI, Deutschland)
- Kritischer Umgang bei E-Mails und Downloads
  - Weitere Informationen im Merkblatt Sichere E-Mails
  - Informationen zu Schadsoftware auf Webseiten und Schadsoftware in E-Mails sowie Spam und Phishing der Melde- und Analysestelle Informationssicherung (MELANI)
- Firewall aktivieren und Virenschutzsoftware installieren
  - Weitere Informationen in der Checkliste PC-Sicherheit
- Sicheres Master-Passwort verwenden
  - Weitere Informationen zu Passwörter des BSI
  - Weitere Informationen und Passwortcheck auf passwortcheck.ch

Trojaner bleiben trotz dieser technischen Massnahmen ein nicht vernachlässigbares Risiko. Passwörter für sensible Dienste (zum Beispiel E-Banking, Paypal oder E-Mail-Dienste) sollen deshalb auf keinem IT-System abgespeichert oder die Zugänge mit einer starken Authentifizierung (zum Beispiel SMS, Google Authenticator, Yubikey, RSA Token) geschützt sein.

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh