

PASSWORTMANAGER IM TEST

Alle Schlüssel für die Cloud

Passwort-Manager sind nur dann praktisch, wenn die Schlüssel auf allen Geräten immer sofort und einfach griffbereit sind. Moderne Cloud-Dienste bieten genau das: clevere SmartphoneApps, versierte Browser-Plugins und eine schnelle Synchronisierung der Login-Daten. ■ WOLF HOSBACH

Ein anonymer Hacker erbeutete letzten Oktober beim beliebten Streamingdienst Twitch 125 Gigabyte an Daten: alle Quellen, alle Projekte, alle Abrechnungsdaten und alle Logins der Anwender. Das gesamte Paket veröffentlichte er in einem Forum, sodass andere Datendiebe beginnen konnten, die Passwörter zu entschlüsseln – bei schwachen Passwörtern ein leichtes Unterfangen. Anwender, die dieselbe Login-Kombination wie bei Twitch auch für andere Dienste nutzten, mussten teilweise feststellen, dass

auch diese Konten schnell geknackt waren. Twitch ist aufgrund der allumfassenden Datenmenge ein spektakulärer, aber bei Weitem kein Einzelfall. Fast alle Internet-Dienste wurden in ihrer Geschichte bereits Opfer von Login-Dieben. Grund genug für uns, die aktuellen Passwort-Manager unter die Lupe zu nehmen, die einen sicheren Umgang mit Login-Daten ermöglichen. Im Unterschied zum letzten Test haben wir die Kriterien diesmal in Richtung Smartphone und Browser verschoben, da wir

davon ausgehen, dass immer weniger Anwender einen stationären Windows-Client verwenden. Als einzige Ausnahme haben wir Keepass XC im Testfeld belassen, quasi als kostenlosen und soliden Vertreter der Windows- und Linux-Clients. Mit Drittanbieter-Apps lässt sich Keepass XC auch cloudfähig machen. Nicht im Test sind ferner die Tools der AV-Hersteller (wie ID Protection von F-Secure oder True Key von McAfee), da wir sie in einer der kommenden Ausgaben eigens untersuchen werden.

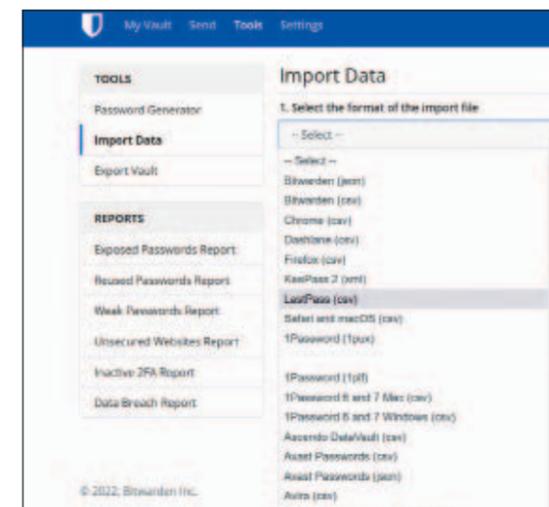
Bild: Elena Abrazhevich / Shutterstock.com

1 Password – praktisch, aber wirr in der Bedienung

Der Passwort-Dienst von Agile Bits liefert insgesamt kein schlechtes Ergebnis, zeigt sich in der Nutzerführung aber oft wirr. Nach wie vor muss der Anwender seine Domäne kennen (also .com oder .eu), wobei die automatischen Umleitungen besser funktionieren als im letzten Test. Neben dem eigentlichen Masterpasswort gibt es noch einen Secret Key, mit dem aber relativ offen umgegangen wird, und der nicht die Kriterien einer Zweifaktorenauthentifizierung (2FA) erfüllt. An der Bedienung hat uns ferner nicht gefallen, dass der Anwender bei der Eingabe von Login-Daten im Web noch einmal klicken muss. Da agieren andere Dienste flüssiger. Andererseits macht 1 Password viele Dinge sehr gut. Zum Beispiel hat der Import unserer Keepass-CSV-Datei problemlos funktioniert. Dann weist der Watchtower nicht nur auf unsichere Passwörter hin, sondern auch auf Dienste, bei denen 2FA möglich wäre, vom Anwender aber nicht eingerichtet ist. Einzigartig ist ferner der Reisemodus, in dem der Nutzer mit einem Klick alle angemeldeten Geräte trennen kann, um Passwörter an Zoll oder Immigration nicht preisgeben zu müssen.

Bitwarden – verdienter Testsieger

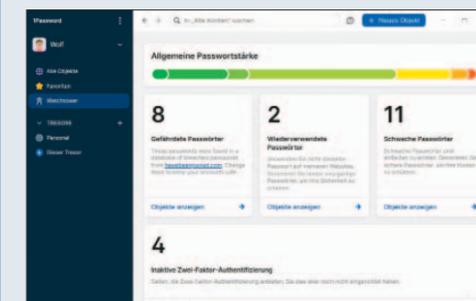
Im letzten Test war der Open-Source-Dienst Bitwarden schon knapp am Testsieger dran, es



Testsieger Bitwarden glänzt mit vielfältigen Importmöglichkeiten, die im Test auch sehr gut funktionierten.

TESTVERFAHREN PASSWORTMANAGER

Im Test spielen drei Kriterien eine Rolle: Sicherheitsfunktionen, Ausstattung und Bedienung. Zur Sicherheit zählen eine Ende-zu-Ende-Verschlüsselung und sichere Anmeldeverfahren. Außerdem sollen die Programme in allen Varianten (Client, App, Addon) Passwörter aus der Zwischenablage wieder löschen. Alle getesteten Tools verfügen inzwischen auch über eine Leak-Überwachung, die meldet, wenn geknackte Login-Daten in irgendeinem Hacker-Forum oder bei Telegram aufgetaucht sind. Bei der Bedienung soll insbesondere der automatisierte Login flüssig erfolgen. Sprich: Das Addon oder die App soll das Eingeben von Nutzerdaten erkennen, diese abgreifen und beim nächsten Mal wieder ausfüllen. Da hakt es leider in vielen Fällen immer noch.



Vorbildlich: 1 Password bewertet Passwort-Qualitäten und zeigt sogar wo 2FA möglich wäre, aber fehlt.



Wolf Hosbach, Redakteur PC Magazin

FAZIT Bei keinem der getesteten Produkte konnten wir gravierende Sicherheitsmängel feststellen, alle verwenden eine solide Ende-zu-Ende-Verschlüsselung, und alle erhalten die Note gut – bis auf den Testsieger, der mit sehr gut abschneidet. Der Anwender kann letztendlich getrost nach Geschmack und Bedienbarkeit entscheiden. Hier stechen in unserem Test insbesondere Bitwarden und Dashlane positiv heraus. Den Testsieger Bitwarden gibt es sogar in einer brauchbaren Gratisvariante. Lastpass, unser Sieger aus dem letzten Jahr, hat etwas nachgelassen. Für Freunde der Cloud-freien Clients ist Keepass XC nach wie vor eine gute Alternative.

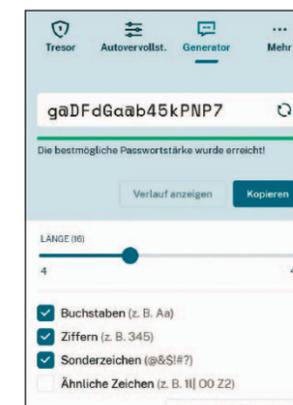
gab aber noch Mängel in der Bedienung, insbesondere beim Login. Diese hat Bitwarden jetzt beseitigt, und Logins funktionierten im Test überall flüssig und schnell. Sehr gut klappte auch der Import von CSV-Daten, was insbesondere für Programmwechsler

interessant ist. Das hier getestete Premium ist darüber hinaus mit neun Euro im Jahr sehr günstig. Zudem gibt es sogar eine kostenfreie Variante, bei der der Anwender auf 2FA, Einmalpasswörter (TOTP) und den Notfallzugriff verzichten muss.

Ein paar Kleinigkeiten müssen wir dennoch bemängeln: Beim Zweischritt-Login (Google, Microsoft usw.) klappte das erstmalige Aufgreifen des Passworts nicht, nur das spätere Ausfüllen. Außerdem war das automatische Löschen der Zwischenablage im Windows-Client nicht voreingestellt. Das führte zu kleineren Punktabzügen.

Dashlane – Meister des automatischen Logins

Ein Bonus des französischen Diensts sind seine europäischen Wurzeln und die entsprechende Datenlagerung – obgleich alle getesteten Systeme eine Ende-zu-Ende-Verschlüsselung betreiben, sodass auch hier die Dienste selbst (und die CIA) keinen Zugriff auf die Daten bekommen können. Top



Anwender können bei vielen Passwort-Generatoren (hier Dashlane) leicht zu verwechselnde Zeichen (wie i und 1 oder 0 und 0) ausschließen.

ist Dashlane in puncto Bedienung: Das Tool hat sämtliche Login-Aufgaben fehlerfrei gemeistert, inklusive des HTTP-Logins – als einziger Kandidat im Testfeld. Wer einen stressfreien Passwortmanager sucht, ist mit dem im Vergleich etwas teureren Dashlane gut beraten. Kleinere Abzüge gab es zum Beispiel für den misslungenen Import des CSV-Daten oder das Nichlöschen der Zwischenablage im Browser-Addon.

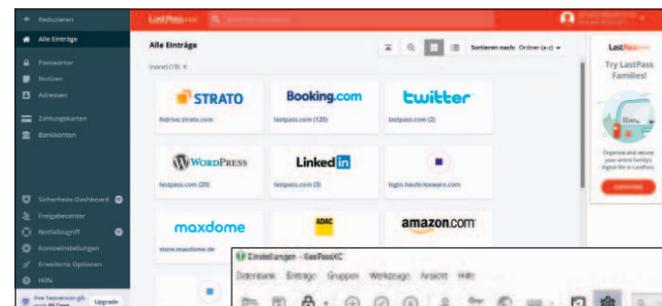
Keepass XC – Client für Windows oder Linux

Das Open-Source-Tool ist das einzige im Test, das keinen Synchronisationsdienst betreibt. Es gibt zwar ein inzwischen gut funktionierendes Browser-Addon und auch passende Smartphone-Apps von Drittanbietern. Die Synchronisation zu diesen App erfolgt dann über Sync-Dienste wie Dropbox oder Google Drive. Mit einer zusätzlichen Schlüsseldatei (die man von Hand verteilt und nicht über Dropbox!) ist das zwar sicher – aber doch eine umständliche Notlösung. Seine Stärken spielt Keepass XC eben als Client aus, zum Beispiel mit den vielfältigen Möglichkeiten der Anmeldung per zusätzlicher Schlüsseldatei (wiederholt) oder Hardware-Token. Auch wer der Ende-zu-Ende-Verschlüsselung der Cloud-basierten Konkurrenten misstraut, findet in Keepass XC

eine gute, internetfreie Lösung. Das Handling erfolgt relativ flüssig, auch im Zusammenspiel mit dem Browser-Addon (falls der Client immer geöffnet ist). Die Oberfläche bietet vielfältige Funktionen und Optionen, was den Einstieg für Anfänger etwas erschwert.

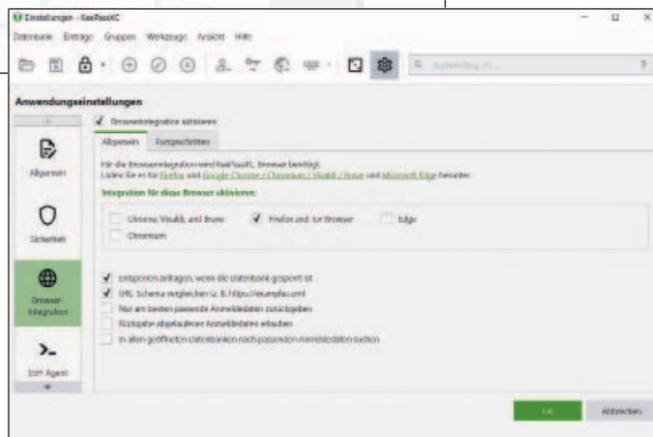
Lastpass – kleine Mängel im Detail

Unser Testsieger des Vorjahrs hat sich offensichtlich auf seinen Lorbeeren ausgeruht, denn in der aktuellen Version stellten wir viele kleine Mängel fest. Ein paar Beispiele: Der Zweischritt-Login hat bei Google gar nicht funktioniert, weder das Aufgreifen der Passwörter noch der Login. Der CSV-Import ist nach wie vor mangelhaft, und einen automatisierten Login in Apps auf dem Smartphone konnten wir nicht nachweisen (mit mehreren Testgeräten). Einmalpasswörter (TOTP) beherrscht Lastpass zwar, jedoch ohne QR-Code-Scannen, was auf dem Smartphone ein Einfaches wäre. Und die App löscht die Zwischenablage mit Passwörtern auf dem Handy nicht. Diese Mängel führten in allen Bereichen zu Punktabzügen und drängten den Cloud-Passwort-Pionier auf Platz drei. Insgesamt erzielt Lastpass aber nach wie vor ein gutes und stabiles Ergebnis.



Die Web-Oberfläche von Lastpass ist übersichtlich und nutzerfreundlich gestaltet.

Keepass XC bietet sehr viele Optionen – gut für den Profi, aber oft verwirrend für den Anfänger.



PASSWORTMANAGER



HERSTELLER	1 BITWARDEN	2 DASHLANE	3 LOGMEIN	4 AGILE BITS	5 OPEN SOURCE
Produkt	Bitwarden Premium 1.32.1	Dashlane Premium 6.2204.3	Lastpass Premium 5.7.0	1Password 8.6.1	KeepassXC 2.7.0
GESAMTWERTUNG	91 Punkte (sehr gut)	84 Punkte (gut)	81 Punkte (gut)	79 Punkte (gut)	78 Punkte (gut)
Preis/Leistung	sehr gut	befriedigend	befriedigend	befriedigend	sehr gut
Preis für 1 Jahr in Euro	9 Euro	39,96 Euro	34,80 Euro	31,80 Euro	kostenlos
SICHERHEITSFUNKTIONEN (MAX. 35 PUNKTE)	33 Punkte	29 Punkte	28 Punkte	28 Punkte	32 Punkte
Algorithmen	AES 256 mit PBKDF2	AES 256 mit Argon2d (u.a.)	AES 256 mit PBKDF2	AES 256 mit PBKDF2	AES 256 mit Argon2d (u.a.)
Ende-zu-Ende-Verschlüsselung	✓	✓	✓	✓	keine Cloud
Open Source	✓	–	–	–	✓
Passwortstärke Masterpasswort	✓ (nur Länge)	✓	✓	✓	–
2-Faktor-Authentifizierung immer / fremde Rechner	✓ (App, Yubikey, Mail, SMS) / ✓	✓ / ✓	✓ (TOTP, Yubikey) / ✓	✓ / ✓	✓ (Schlüsseldatei, HW-Token) / entfällt
PW-Leak-Überwachung	✓	✓	✓	✓ (nicht voreingestellt)	✓
PW-Qualitätsprüfung in Datenbank	✓	✓	✓	✓	✓
Passwortgenerator / lesbare PWs	✓ / ✓	✓ / ✓ (nur im Plugin)	✓ / ✓	✓ / –	✓ / ✓
Einmalschlüssel (TOTP) / mit QR-Code	✓ / ✓ (App)	✓ / ✓	✓ / –	✓ / ✓ (versteckt)	✓ / –
Windows Client					
automatisches Schließen / Löschen Zwischenablage	✓ / ✓ (nicht voreingestellt)	entfällt	entfällt	✓ / ✓	✓ / ✓
Browser-Plugin					
Masterpasswort bei bestimmten Seiten (Banken)	–	✓	✓	–	entfällt
automatisches Schließen / Löschen Zwischenablage	✓ / ✓	✓ / –	✓ (nicht voreingestellt) / ✓	✓ / –	entfällt
Länder sperren	–	–	✓ (auch Tor)	–	entfällt
SmartphoneApp					
Biometrie-Login	✓	✓	✓	✓	entfällt
Screenshot verhindern	✓	✓	✓	✓	entfällt
automatisches Schließen / Löschen Zwischenablage	✓ / ✓	✓ / ✓	✓ / –	✓ / ✓ (nicht voreingestellt)	entfällt
AUSSTATTUNG (MAX. 30 PUNKTE)	27 Punkte	20 Punkte	24 Punkte	25 Punkte	14 Punkte
Client Windows / Linux / portable	✓ / ✓ / ✓	–	–	✓ / ✓ / –	✓ / ✓ / ✓
Browser-Plugins Chrome (Edge, Opera) / FF	✓ / ✓	✓	✓ / ✓	✓ / ✓	✓ / ✓
App Android / iOS	5.0 / 10.0	8.0 / 14	5.0 / 13.0	5.0 / 12	– (aber Drittanbieter)
Synchronisation Cloud	✓	✓	✓	✓	–
Webzugriff auf Passwörter	✓	✓	✓	✓	–
Import CSV / Chrome / FF / Keepass	✓ (und viele mehr)	CSV	✓ / ✓ / – / ✓ (viele mehr)	✓ (und viele mehr)	✓ / – / – / ✓
Export	JSON, CSV	CSV	CSV (über E-Mail)	CSV	CSV, Html
Notfallzugriff / Kontowiederherstellung	✓	✓	✓	–	–
Datenbank bereinigen und Duplikate finden	–	–	✓	–	–
BEDIENUNG (MAX. 35 PUNKTE)	31 Punkte	35 Punkte	29 Punkte	26 Punkte	32 Punkte
Auto Login speichern	✓	✓	✓	✓ (mit Klick)	✓ (mit Klick und etwas wirr)
Auto Ausfüllen	✓ (nicht aktiviert)	✓	✓	✓ (mit Klick)	✓
Zweischritt-Login (Google)	✓ (nur ausfüllen)	✓	✓ (Fehler bei Google)	✓ (mit Klick)	✓
http-Login	–	✓ (!)	–	–	–
App: Login Web / Login andere Apps	✓ / ✓	✓ / ✓	✓ / –	✓ / ✓	entfällt
FAZIT					
	Als Open-Source-Tool erfüllt Bitwarden hohe Sicherheitsstandards. Zudem ist es funktionsreich und inzwischen sehr nutzerfreundlich.	Der französische Dienst Dashlane erhält im Test für die Bedienung die volle Punktzahl. Dafür ist sein Preis etwas höher.	Im Vergleich mit dem Test des Vorjahrs fanden wir kleinere Mängel bei Lastpass. Insgesamt zeigt sich der Dienst aber stabil und anwenderfreundlich.	1 Password bietet viele gute Ideen (wie den Reisemodus), die Bedienung ist aber nicht so flüssig wie bei den Konkurrenten und wirkt oft etwas unklar.	Als stationäres Open-Source-Tool macht Keepass XC einen exzellenten Job, kann insgesamt mit den Cloud-Diensten aber nicht mithalten.