Bild: Thorsten Hübner

Goodbye, LastPass

So wechseln Sie zum Passwortmanager KeePassXC

LastPass schränkt die Gratisnutzung ein. Jetzt bietet sich ein Wechsel zu KeePassXC an, das nicht nur Open Source ist, sondern mithilfe von Syncthing auch ohne Cloud synchronisiert.

Von Jan Schüßler

Zum 16. März zieht LastPass die Schrauben bei der Gratisversion seines Passwortmanagers an: Sie lässt sich künftig nur noch entweder auf mobilen Geräten oder auf Desktops nutzen. Wer weiterhin zwischen beiden Gerätekategorien synchronisieren will, braucht mindestens die Premiumversion für 35 Euro im Jahr. Doch neben den Kosten gibt es einen weiteren Grund für einen Umstieg: Wie unser Privatsphäre-Test [1] vor ein paar Wochen gezeigt hat, tracken nicht nur LastPass, sondern auch diverse andere Anbieter von Passwortmanagern ihre Kunden recht schamlos.

Einen hervorragenden Schutz vor Tracking – und vor der Abhängigkeit von einem Hersteller – bieten quelloffene Passwortmanager aus dem KeePass-Universum. In unserer Anleitung konzentrieren wir uns auf Windows und Android, geben aber auch iOS-Nutzern ein paar Tipps. Auf dem Windows-Desktop haben wir uns für KeePassXC entschieden, weil es sich um einiges komfortabler bedienen lässt als das reguläre KeePass. Auf Android kommt KeePassDX zum Einsatz. Eine Kernfunktion von LastPass ist die komfortable Synchronisierung des Passworttresors zwischen mehreren Geräten. Für diese Aufgabe verwenden wir die quelloffene Sync-Software Syncthing. Sie kommt ohne Cloudspeicher aus und funktioniert trotzdem auch unterwegs, über NAT-Grenzen hinaus.

Export aus LastPass

Um den Umstieg so elegant wie möglich hinzubekommen, exportieren Sie zunächst die in LastPass eingetragenen Passwörter als CSV-Datei, die alle gespeicherten Log-in-Daten im Klartext enthält. Aus der Weboberfläche heraus ist der Export seit geraumer Zeit kaputt und zeigt die Passwörter nur als Text im Browser an, statt sie herunterzuladen. Der Weg des Erfolgs führt deshalb über die LastPass-Browsererweiterung. Klicken Sie im Menü der Erweiterung auf „Kontooptionen/Erweitert/Exportieren/Lastpass-CSV-Datei“.

Am besten speichern Sie die CSV-Datei auf einem verschlüsselten Laufwerk ab. Falls Ihr Systemlaufwerk nicht verschlüsselt ist, können Sie auch einen verschlüsselten USB-Stick dafür benutzen, wie wir ihn in [2] beschrieben haben. So stellen Sie sicher, dass nach dem späteren Löschen der Datei keine zum Beispiel für einen Dieb des PCs verwertbaren Rückstände auf der Systemfestplatte beziehungsweise -SSD zurückbleiben – immerhin enthält sie Ihre Passwörter im Klartext.

KeePassXC: Ersteinrichtung

Laden Sie nun KeePassXC herunter (siehe ct.de/y5ce) und installieren und starten Sie es. Klicken Sie auf „Aus CSV importieren“ und wählen Sie die zuvor gesicherte Datei lastpass_export.csv aus. Als Nächstes können Sie einen Namen für die Passwortdatenbank vergeben oder die Vorgaben einfach bestätigen. Glei-

ches gilt für die Verschlüsselungseinstellungen.

Dann vergeben Sie ein starkes Masterpasswort nach den bekannten Regeln: nicht zu kurz und nicht einfach zu erraten. Um die Sicherheit zu erhöhen, ohne das Masterpasswort endlos lang und kompliziert machen zu müssen, empfiehlt es sich, eine Schlüsseldatei als zweiten Faktor hinzuzunehmen. In diesem Fall fragt KeePassXC beim Öffnen eines Passworttresors nicht nur nach dem Masterpasswort, sondern verlangt auch nach der Schlüsseldatei. Auch wenn jemand Ihre Passwortdatenbank (eine Datei mit der Endung .kdbx) klaut und Ihr Masterpasswort ausspäht, fehlt immer noch die Schlüsseldatei. Auf die Datei sollten Sie gut aufpassen und sie keinesfalls an einem öffentlich zugänglichen Ort speichern. Kopieren Sie sie am besten auf direktem Wege, also etwa per USB-Stick oder -Kabel, auf die Geräte, mit denen Sie auf den Passworttresor zugreifen möchten. Sie können KeePassXC eine Schlüsseldatei erzeugen lassen, aber Sie können auch eine beliebige, schon vorhandene Datei nehmen. Ideal ist irgendein Handyfoto, das Sie nirgendwo veröffentlicht haben – es ist unauffällig und quasi garantiert einmalig. Um die Sicherheit noch weiter zu erhöhen, legen Sie Ihre Schlüsseldatei nicht direkt auf dem PC ab, sondern auf einem verschlüsselten USB-Stick, den Sie immer dabei haben [2].

Um Chaos bei der späteren Synchronisierung zu vermeiden, empfehlen wir im nächsten Schritt, die Datei nicht einfach im Dokumentenordner, sondern in einem eigenen Unterordner zu speichern. Den legen Sie per Rechtsklick in den freien Bereich des Fensters und „Neu/Ordner“ an. Nennen Sie ihn zum Beispiel „Passwortordner“, öffnen Sie ihn und bestätigen Sie mit „Speichern“.

Jetzt folgt der eigentliche Import Ihrer Passwörter. Weil KeePassXC nicht wissen kann, wie die Einträge der CSV-Datei sortiert sind, müssen Sie ihm mitteilen, was was ist. Setzen Sie im Bereich „Zeichensatz“ ein Häkchen vor „Erste Zeile enthält Feldnamen“. Sortieren Sie dann die Spalten unter „Spalten-Zuordnung“: Gruppe=grouping, Titel=name, Benutzername=username, Passwort=password, URL=url, Notizen=extra. Die restlichen vier Felder setzen Sie auf „Nicht vorhanden“.

Falls in der LastPass-Datenbank auch Einträge liegen, die keine Passwörter sind – also etwa Notizen, Kreditkartendaten oder Formulardaten –, werden die ebenfalls übernommen. Der Nutzen hält sich in Grenzen, denn KeePassXC unterstützt solche Datensätze nicht und interpretiert sie einfach als Passworteinträge. Zwar kann man mit einigem Aufwand händisch Einträge mit benutzerdefinierten Feldern für Kartennummern, Anschriften oder Telefonnummern erstellen und befüllen, doch beim CSV-Import stopft KeePassXC Kreditkarten & Co. einfach ins Passwortschema. Wir empfehlen daher, diese Importe zu löschen und solche Einträge bei Bedarf von Hand neu anzulegen.

Komfort im Browser

Sie könnten KeePass XC nun direkt verwenden, doch die Bedienung im Alltag wäre noch ein wenig sperrig, weil Sie Webseiten-Passwörter jedes Mal umständlich aus dem Programm heraus aufrufen müssten. Diese Arbeit nimmt Ihnen eine Browsererweiterung ab. Es gibt sie sowohl für Firefox als auch für Chrome (und damit auch für Chromium-Browser wie Brave, Edge, Vivaldi & Co.). Nur Safari geht leer aus.

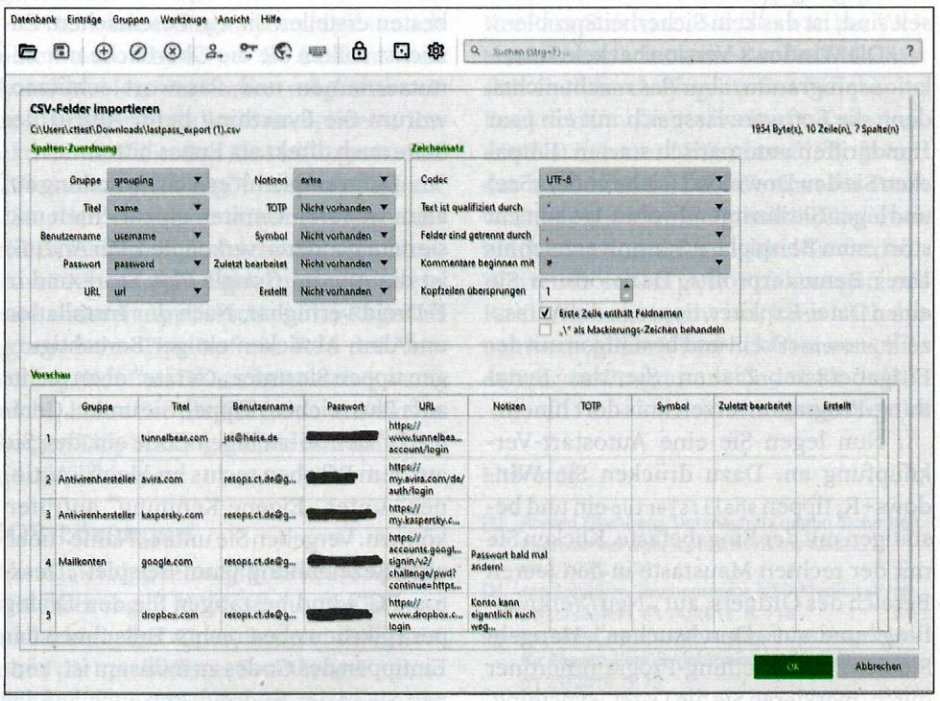
Die Funktion aktivieren Sie über die „Einstellungen“ im Menü „Werkzeuge“. Wählen Sie links „Browserintegration“, setzen Sie das Häkchen vor „Browserintegration aktivieren“ sowie vor Ihren Browser und laden Sie die passende Erweiterung über den dazugehörigen Link herunter, der sich direkt darüber befindet. Bestätigen Sie die Einstellungen mit OK. Klicken Sie nun im Browser auf die Erweiterung – im Regelfall oben rechts im Fenster – und dann auf „Verbinden“. In der Verbindungsanfrage vergeben Sie einen Namen wie „Desktop-Firefox“.

Beim Aufruf von Webseiten, für die KeePassXC Logindaten kennt, sollte nun automatisch eine Zugriffsanfrage im Browser erscheinen, um Benutzername und Passwort einzutragen. Sofern Sie diese Anfrage nicht bei jedem Aufruf der Seite erneut sehen möchten, setzen Sie ein Häkchen bei „Merken“. So oder so lassen sich die Login-Daten dann per Klick auf das kleine KeePassXC-Icon im Benutzernamenfeld eintragen.

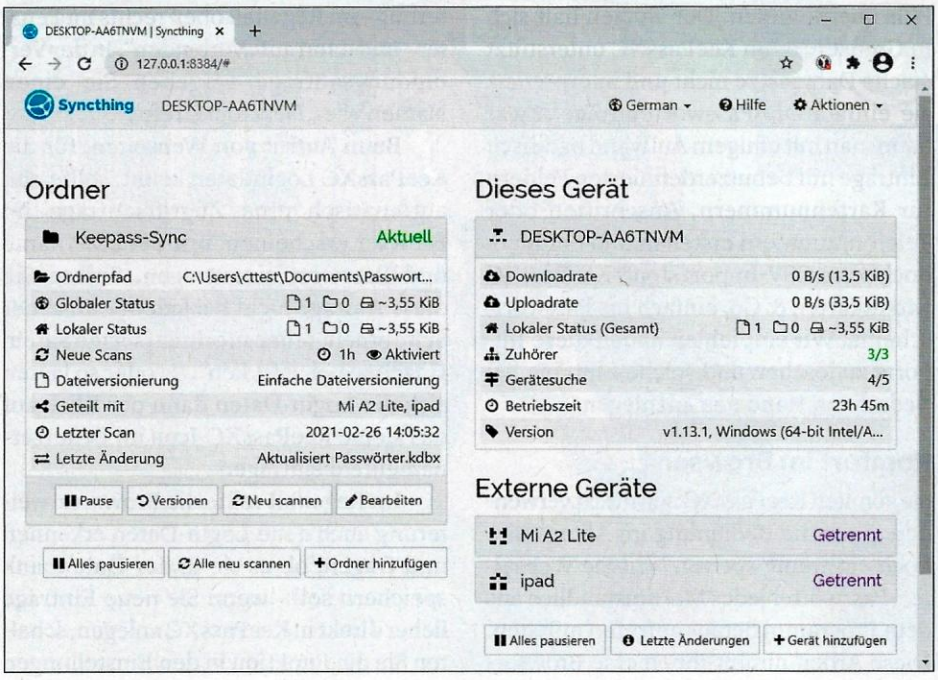
Im Regelfall sollte die Browsererweiterung auch neue Login-Daten erkennen und fragen, ob es sie in der Datenbank speichern soll – wenn Sie neue Einträge lieber direkt in KeePassXC anlegen, schalten Sie die Funktion in den Einstellungen der Browsererweiterung ab (per Klick aufs Erweiterungs-Icon und „Einstellungen“). Dort können Sie noch mehr einstellen, etwa, ob Login-Daten automatisch eingetragen und/oder abgeschickt werden.

Sync ohne Cloud

Wie kommt die Passwortdatenbank nun auf andere Geräte? Die bequemste Lösung wäre es, sie einfach im lokalen Ordner eines Cloudspeichers wie Dropbox oder OneDrive abzulegen. Das wäre zwar auch sicher, würde aber wieder ein Konto bei einem Cloudanbieter erfordern.



Die Importfunktion von KeePassXC übernimmt Ihre Passwortliste problemlos – die Spalten müssen nur passend sortiert werden.



Einmal eingerichtet, verrichtet Syncthing seinen Dienst unauffällig im Hintergrund.

Die Lösung ist Peer-to-Peer-Synchronisierung (P2P), wofür wir das quelloffene Tool Syncthing verwenden. Damit sich Geräte auch über NAT-Grenzen hinweg finden und synchronisieren können, betreibt Syncthing Discovery-Server, die die Verbindung vermitteln. Zudem existieren weltweit ein paar hundert Community-gestützte Relay-Server, die als Proxy arbeiten, falls Daten nicht auf direktem Wege ausgetauscht werden können. Da die Übertragungen Ende-zu-Ende-verschlüsselt sind, ist das kein Sicherheitsproblem.

Die Windows-Version hat kein Installationsprogramm, aber das macht nichts, denn die Software lässt sich mit ein paar Handgriffen automatisch starten. Entpacken Sie den Download (siehe ct.de/y5ce) und legen Sie ihn irgendwohin, wo er nicht stört, zum Beispiel ins Stammverzeichnis Ihres Benutzerprofils. Dazu öffnen Sie einen Datei-Explorer, tippen in die Adresszeile `%homepath%` ein und bestätigen mit der Eingabetaste. Ziehen Sie das Syncthing-Programmverzeichnis dort hinein.

Nun legen Sie eine Autostart-Verknüpfung an. Dazu drücken Sie Windows+R, tippen `shell:startup` ein und bestätigen mit der Eingabetaste. Klicken Sie mit der rechten Maustaste in den leeren Bereich des Ordners, auf „Neu/Verknüpfung“ und auf „Durchsuchen“. Hangeln Sie sich zum Syncthing-Programmordner durch, markieren Sie die Datei „syncthing.exe“ und bestätigen Sie mit OK. Ergänzen Sie die Pfadzeile noch um ein Leerzeichen gefolgt von `-no-console -no-browser`, und klicken Sie die Dialoge bis zum Ende durch.

Geräte verknüpfen

Um die Synchronisierung einzurichten, rufen Sie das Programm syncthing.exe in seinem Programmordner per Doppelklick auf und bestätigen eine eventuelle Firewall-Abfrage. Die Konfiguration geschieht per Browser und ist jederzeit unter der Adresse `127.0.0.1:8384` erreichbar – am besten erstellen Sie ein Lesezeichen. Zunächst sollten Sie die Oberfläche mit Benutzernamen und Passwort schützen, worum Sie Syncthing beim Aufruf der Seite auch direkt als Erstes bittet.

Dann empfiehlt es sich, Syncthing auf allen weiteren Geräten einzurichten und sie miteinander zu verknüpfen. Für Android ist die App im Google Play Store und in F-Droid verfügbar. Nach der Installation und dem Abnicken einiger Berechtigungen tippen Sie unter „Geräte“ oben rechts aufs Pluszeichen. Tippen Sie unter „Geräte-ID“ den 56-stelligen Code ein, den Sie auf dem PC oben rechts im Menü „Aktionen“ unter „Eigene Kennung“ aufrufen können. Vergeben Sie unter „Name“ noch eine Bezeichnung (zum Beispiel „Desktop-PC“) und bestätigen Sie den Dialog per Häkchen oben rechts. Falls Ihnen das Eintippen des Codes zu mühsam ist, können Sie in der Android-App auch auf das kleine QR-Code-Logo in der Zeile „Geräte-ID“ tippen und einfach den Code scannen, den Sie auf dem Desktop ebenfalls sehen.

Auf dem Desktop-Rechner erscheint das Gerät jetzt im besten Fall schon automatisch auf der Hauptseite, wo man es per Klick hinzufügen kann. Wenn nicht: Im Bereich „Externe Geräte“ auf „Gerät hinzufügen“ klicken und unter „Gerätekennung“ den 56-stelligen Gerätecode eingeben, den Sie im Menü der Android-App (die drei Striche oben links) unter „Geräte-ID anzeigen“ aufrufen können.

Falls Ihre Geräte im gleichen Subnetz hängen (etwa zu Hause am DSL-Router), finden sie sich übrigens meist schon von selbst, was Ihnen das Eintippen oder Abscannen der Geräte-ID erspart. Schauen Sie einfach auf dem Desktop nach, ob Syncthing IDs potenzieller Gegenstellen im Hinzufügedialog vorschlägt.

Datenbank synchronisieren

Sind alle Geräte verbunden, klicken Sie in Syncthing auf dem PC im Bereich „Ordner“ auf „Ordner hinzufügen“. Tragen Sie auf der Registerkarte „Allgemein“ im Feld „Ordnerkennung“ einen eindeutigen Namen ein, zum Beispiel „KeePass-Sync“. Unter „Ordnerpfad“ tragen Sie den Ordner ein, in dem Ihre Passwortdatenbank liegt, also etwa „C:\Users\cttest\Documents\Passwortordner“. Syncthing bietet leider keinen Dialog für die Ordnerauswahl – statt den Pfad von Hand einzutippen, können Sie den Ordner mit der Datenbank im Explorer öffnen und dort auf die Adresszeile klicken. So lässt sich der Pfad einfach kopieren und in Syncthing einfügen. Die „Ordnerbezeichnung“ kann leer bleiben.

Auf der Registerkarte „Teilen“ setzen Sie Häkchen vor alle Geräte, zwischen denen die Passwortdatenbank synchronisiert werden soll. Zu guter Letzt können Sie unter „Dateiversionierung“ einstellen, dass ältere Versionen der Datenbankdatei eine Zeit lang aufbewahrt werden. Sinnvoll ist die „Einfache Dateiversionierung“ mit automatischem Löschen nach 14 Tagen und Aufbewahrung von bis zu 100 alten Versionen. Bestätigen Sie nun mit „Speichern“.

Auf einem Android-Gerät sollte Ihnen nun eine Benachrichtigung mitteilen, dass der Desktop-PC einen Ordner mit Ihnen teilen möchte. Tippen Sie sie an. Sie sehen einen fast fertig ausgefüllten Dialog für einen synchronisierten Ordner – fast, weil Syncthing in der Zeile „Verzeichnis“ noch wissen möchte, in welchem lokalen Ord-

ner es die Passwörter synchronisieren soll. Wir empfehlen, in dem von der App vorgeschlagenen Download-Ordner einen Unterordner zu erstellen und auszuwählen – denn andernfalls landen sämtliche Inhalte des Download-Ordners auch auf Ihren anderen Geräten. Stellen Sie auch hier auf Wunsch noch eine Versionierung ein und bestätigen Sie oben rechts per Tipp aufs Häkchen.

Ob der Sync funktioniert, können Sie nun in der Dateimanager-App Ihres Smartphones prüfen. Im synchronisierten Unterordner sollte sich nach kurzer Wartezeit Ihre KDBX-Datei befinden.

KeePass auf Android

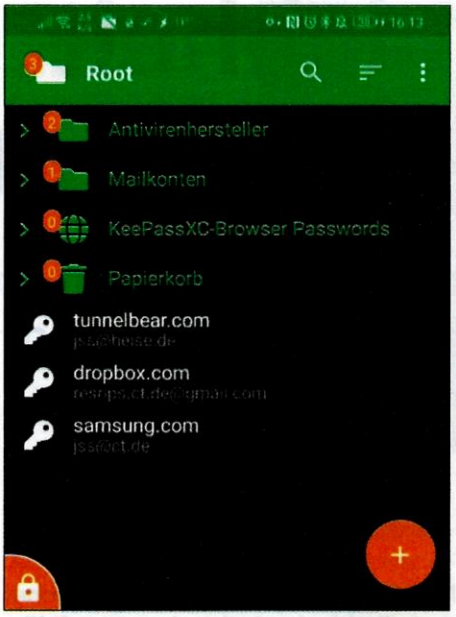
Unter den diversen Apps, die die KeePass-Community entwickelt hat, besteht im Prinzip freie Auswahl, solange sie mit dem KDBX-Format umgehen können. Wir haben uns für KeePassDX entschieden. Es ist sowohl im Play Store als auch in F-Droid zu finden.

Vorab sollten Sie die Schlüsseldatei – sofern Sie eine solche zusätzlich zum Masterpasswort zum Öffnen des Passworttresors verwenden – aufs Smartphone kopieren. Im Idealfall erledigen Sie das per lokaler Verbindung (Datenkabel) und legen sie in einem Ordner ab, der nicht in irgendeiner Weise synchronisiert wird. Beim Öffnen von KeePassDX binden Sie nun den Passworttresor per Tipp auf „vorhandene Datenbank öffnen“ und Auswahl der KDBX-Datei ein. Tippen Sie das Masterpasswort ein und teilen Sie der App gegebenenfalls mit, wo die Schlüsseldatei liegt. Um künftig den Fingerabdrucksensor statt des Masterpassworts zu benutzen, tippen Sie nach Eingabe von Passwort und Schlüsseldatei nicht unten auf „Öffnen“, sondern auf das orangene Fingerabdruck-Logo.

Automatisch ausfüllen

Wie andere mobile Passwortmanager hilft auch KeePassDX beim Ausfüllen von Login-Feldern im Browser und anderen Apps. Dafür stehen zwei Funktionen bereit. Zum einen die KeePassDX-Tastatur, genannt Magikeyboard. Um sie zu verwenden, öffnen Sie in KeePassDX die Einstellungen und unter „Formularausfüllung“ die „Gerätetastatur-Einstellungen“. Schalten Sie „Magikeyboard“ ein und bestätigen Sie die Abfragen.

Zum Ausfüllen tippen Sie in ein Login-Feld und schalten die Tastatur auf „Magikeyboard“ um – wie das geht, kann von Gerät zu Gerät verschieden sein; oft gibt



Es gibt so einige KeePass-Apps für Android – KeePassDX ist komfortabel und übersichtlich.

es dafür ein kleines Tastatursymbol unten rechts auf der Navigationsleiste. Tippen Sie dann auf das Schlüsselsymbol, woraufhin sich KeePassDX öffnet. Tippen Sie die Datenbank an, entsperren Sie sie und wählen Sie den passenden Passworteintrag aus. Die App führt Sie zurück zum Browser, wo Sie Benutzername und Passwort einfach nacheinander per Tipp auf das Personen-Icon sowie auf das „***“-Icon einfügen können.

Neben dem Magikeyboard gibts noch einen Autofill-Dienst. Er bedient sich komfortabler, funktioniert möglicherweise aber nicht auf allen Smartphones. Ihn aktivieren Sie in den Einstellungen unter „Formularausfüllung“ mit einem Tipp auf „Standarddienst für automatisches Ausfüllen festlegen“ und Auswahl von „KeePassDX“. In Login-Feldern von Browsern und anderen Apps erscheint im Regelfall schon beim Tipp auf ein Feld der Vorschlag, KeePassDX zu benutzen – wenn nicht, holen Sie die Funktion mit einem langen Tipp ins Eingabefeld und dann auf „Autofill“ hervor.

iOS-Lösungen

Von Syncthing selbst gibt es keine App für iOS, aber es gibt Möbius Sync. Das ist zwar nicht komplett Open Source, integriert aber die quelloffene Syncthing-Engine. Die Bedienung etwa auf einem iPad gleicht der auf dem Desktop nahezu vollständig. Möbius Sync ist zunächst kostenlos, doch wer einen Datenbestand größer als 20 MByte synchronisieren will, muss das für rund 5 Euro freischalten – einmalig, nicht per Abo. Geht es nur um eine Passwortdatenbank, dürfte die Gratisversion meist ausreichen.

Als Passwortmanager für iOS empfehlen sich etwa KeePassium oder Strongbox, die zwar quelloffen sind, aber für den vollen Funktionsumfang per Abo oder Einmalzahlung freigeschaltet werden wollen. Die Einschränkungen im Gratisbetrieb erweisen sich bei Strongbox als etwas lästiger, weil es biometrische Authentifizierung dann zwar zum Öffnen der App, nicht aber zum Öffnen von Passworttresoren erlaubt und jedes Mal das Masterpasswort fällig wird. Die Preise für Monatsabo, Jahresabo und Dauerlizenz liegen für Strongbox bei 3 Euro, 14 Euro und 44 Euro und für KeePassium bei 2 Euro, 15 Euro und 50 Euro.

Anders machen

Diese Anleitung eignet sich nicht nur zum Umstieg von LastPass. Sie können Sie in ähnlicher Weise auf jeden anderen Passwortmanager münzen, von dem Sie loskommen möchten – sehr wahrscheinlich wird es beim CSV-Import hier und dort Unterschiede in der Spaltensortierung geben.

Auch spricht nichts gegen die Verwendung anderer Apps, wenn Sie etwas finden, das Ihnen besser gefällt: Auf dem Smartphone zum Beispiel KeePass2-Android, auf dem Desktop die reguläre KeePass-Software. Sie ist zwar bei Weitem nicht so schick wie KeePassXC, lässt sich aber durch Plug-ins fast beliebig im Funktionsumfang erweitern. Entscheidend ist in erster Linie, dass die Software das quelloffene KDBX-Format für Passwortdatenbanken unterstützt. Und auch bei der Synchronisierung sind Sie flexibel. Wer etwa schon gute Erfahrungen mit Resilio Sync gemacht hat, kann auch das nehmen – einen Überblick über verschiedene Sync-Programme finden Sie in [3].

(jss@ct.de) **ct**

Literatur

[1] Ronald Eikenberg, Datenschutz gegen Sicherheit, Passwortmanager-Apps im Privacy-Check, c't 5/2021, S. 24
[2] Jan Schüßler, Taschentresor, USB-Medien sicher verschlüsseln, c't 14/2018, S. 116
[3] Jan Mahn, Synchrone Satelliten, Vier Programme für Peer-to-Peer-Synchronisation im Test, c't 23/2018, S. 78

Alle Downloads: ct.de/y5ce