Vergessen Sie Ihre Passwörter!

... nachdem Sie diese im unknackbaren Passwortmanager KeePassXC gespeichert haben. Wir zeigen die Einrichtung, den Import von Firefox-Passwörtern und die Handysynchronisation

VON ANDREAS DUMONT

Passwörter sind ein leidiges Thema. Es gibt unzählige Vorgaben und Strategien, und je nachdem, wen Sie fragen, bekommen Sie unterschiedliche Tipps und Ratschläge. Das Ergebnis sind häufig mangelhafte Passwörter, die schlichtweg zu kurz sind. Egal ob mit Sonderzeichen und Großbuchstaben, acht Zeichen sind definitiv zu wenig. Solche Passwörter lassen sich in wenigen Stunden knacken. Doch längere, komplizierte Zeichenfolgen überfordern meist das menschliche Gedächtnis. Dazu kommt: Ein Passwort für mehrere Konten zu verwenden, ist fahrlässig, aber wer kann schon für die unzähligen Webdienste unterschiedliche Passwörter behalten? Wenn Sie sich Ihre Passwörter merken können, dann sind sie vermutlich nicht stark genug, um Ihre Konten zu schützen. Die Lösung ist ganz einfach und nennt sich KeePassXC. Das geniale Programm merkt sich für Sie sämtliche Passwörter und lässt sich universell einsetzen und synchronisieren. Künftig brauchen Sie sich nur noch ein einziges starkes Masterpasswort zu merken.

CHIP PROFI
Insiderwissen für den Technikexperten

KeePassXC einrichten

Das Programm lässt sich wahlweise installieren oder als portable Version nutzen. Im ersten Schritt erstellen Sie eine neue, sicher verschlüsselte Datenbank. Darin speichern Sie alle Benutzernamen, Passwörter, Kontonummern oder PINs für Webseiten, Programme oder andere passwortgeschützte Bereiche. Klicken Sie auf »Neue Datenbank erstellen« und vergeben Sie einen Namen und optional eine Beschreibung. Die Verschlüsselungseinstellungen können Sie auf

ILLUSTRATION: CREATIVE-TOUCH/GETTY IMAGES

Die Software aus diesem Beitrag finden Sie auf der virtuellen CHIP-DVD

E-Paper-Leser können die virtuelle DVD unter **chip-kiosk.de/produkte** nachbestellen

den Standardwerten belassen. Nun gilt es, die Datenbank mit einem sicheren Masterpasswort zu schützen – dem einzigen, das Sie sich künftig merken müssen.

Sie können auch KeePassXC über das Würfelsymbol ein Zufallspasswort erstellen lassen, allerdings nur mit englischen Wörtern. Wie auch immer Sie das Passwort erzeugt haben, tragen Sie es zweimal ein. Wenn Sie auf »Zusätzlichen Schutz hinzufügen« klicken, dann erzeugt das Tool eine Schlüsseldatei, die als zweiter Faktor dient und nicht verloren gehen darf. Sie können die Schlüsseldatei aber auch jederzeit später hinzufügen.

Browser-Plug-in sorgt für Komfort

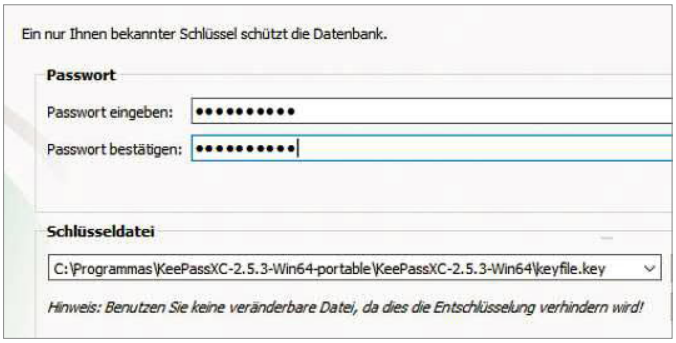
Die Browserintegration sorgt dafür, dass KeePassXC automatisch Benutzernamen und Passwörter in die Anmeldefelder einer Webseite einträgt. Um sie einzurichten, rufen Sie im Menü »Werkzeuge« die Einstellungen auf. Hier wechseln Sie in den Bereich »Browser-Integration« und wählen die Option »Browser-Integration aktivieren«. Setzten Sie ein Häkchen vor den oder die Browser, bei denen Sie das automatische Eintragen von KeePassXC nutzen wollen. Im Browser – z. B. Beispiel Firefox – installieren Sie die Erweiterung: Wechseln Sie zu »Add-ons | Erweiterungen« und suchen Sie nach »KeePass-XC-Browser«. Mit »Zu Firefox hinzufügen« installieren Sie das Add-on. In der Symbolleiste erscheint daraufhin ein zusätzliches Icon. Wenn Sie es anklicken, blendet sich ein kleines Dialogfeld ein. Klicken Sie auf »Verbinden«, um KeePassXC mit dem Browser zu verknüpfen.

Durchblick: Passwörter mit KeePassXC verwalten

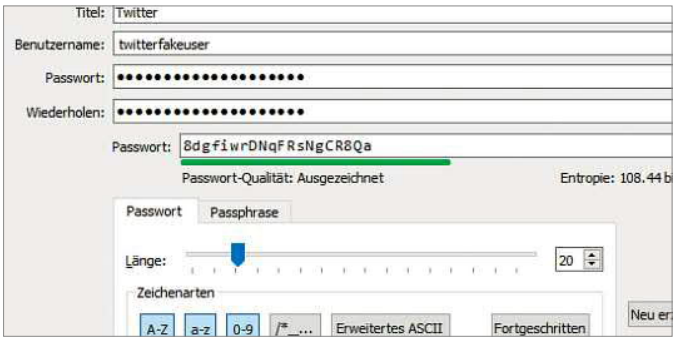
Es empfiehlt sich der Übersichtlichkeit halber, im ersten Schritt mehrere Gruppen anzulegen, etwa »Online-Banking«, »Social Media« oder »Hobbies«. Der naheliegende Weg führt über den Menüpunkt »Gruppe | Neue Gruppe«. Neben dem Namen legen Sie optional ein Verfallsdatum fest. Per Drag & Drop lassen sich Einträge von einer Gruppe in eine andere verschieben.

Um einen neuen Eintrag in den Tresor zu legen, wählen Sie »Einträge | Neuer Eintrag«. Vergeben Sie einen Titel und tragen Sie den Benutzernamen ein. Das Passwort können Sie von KeePass erstellen lassen. Dazu klicken Sie auf das Würfelsymbol. Geben Sie die gewünschte Länge oder die Zahl der Wörter an. Der Entropiewert ist ein Maß, wie gut das Passwort ist. Ein →

KeePassXC erstellt verschlüsselte Datenbanken mit den Zugangsdaten für Webseiten und andere passwortgeschützte Bereiche



Optional lässt sich eine Schlüsseldatei erstellen, die als zweiter Faktor für zusätzliche Sicherheit sorgt



KeePassXC verfügt über einen Passwortgenerator. Passwörter mit einer Entropie von 100 Bit oder mehr sind nicht zu knacken

Firefox-Passwörter importieren

Wer einen Passwortmanager neu anlegt, steht anfangs vor der recht mühsamen Aufgabe, bereits bestehende Passwörter zu erfassen und einzutragen.

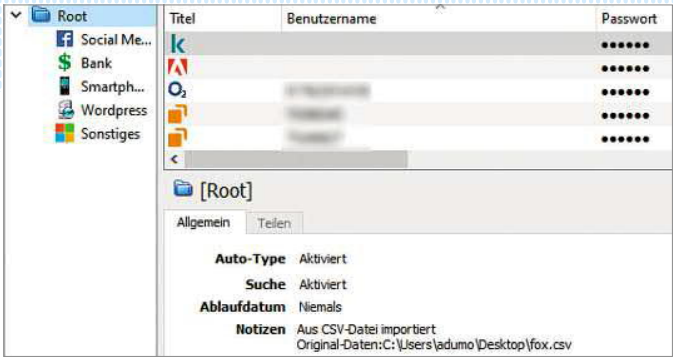
> Der Browser Firefox bietet zwar das praktische Feature an, die Zugangsdaten all Ihrer Onlinekonten zu speichern, verfügt aber über keine Exportfunktion. Hier ist externe Hilfe erforderlich.

> Das Tool PasswordFox kann Passwörter von Firefox auslesen und in einem KeePass-kompatiblen CSV-Format abspeichern. Nach dem Start des Tools sehen Sie alle Log-in-Daten, die Firefox gespeichert hat. Mit »View | Choose Columns« passen Sie die Ansicht entsprechend an. Notwendig sind »Web Site«, »User Name« und »Password«. Mit [Strg] + [A] markieren Sie alle Einträge und exportieren diese mit »File | Save Selected Items«. Als Dateiformat wählen Sie »KeePass csv file«.

> In KeePassXC gehen Sie zu »Datenbank | Importieren | CSV-Datei ...«. Nun müssen Sie die Felder zuordnen. Dazu gehen Sie im Abschnitt »Spaltenlayout« die einzelnen Punkte durch und weisen ihnen die passenden Spalten zu.

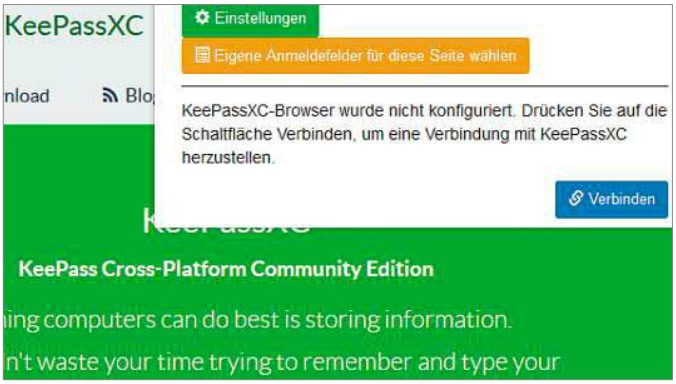
> Das Ergebnis sehen Sie im Vorschaufenster. Ein Klick auf »OK« führt den Import durch. Die CSV-Datei, die ja Klartext enthält, sollten Sie danach löschen.

Vor dem Import der Passwörter aus Firefox muss noch das Spaltenlayout angepasst werden



In KeePassXC lassen sich beliebig viele Gruppen erstellen, was die Verwaltung der Passwörter deutlich übersichtlicher macht

Das Firefox-Add-on ist erforderlich für die Browserintegration von KeePassXC



Über das Icon in der Symbolleiste lässt sich der Browser mit dem Passworttresor verbinden

Die Statistiken zeigen, ob die gespeicherten Passwörter schwach sind oder mehrfach verwendet werden

Passwort mit einer Entropie von 100 oder mehr ist mit den heutigen technischen Möglichkeiten nicht zu knacken. Heraus kommt dann so etwas wie »8dgfiwrDNqFRsNgCR8Qa«, was auch für echte Gedächtniskünstler eine Herausforderung darstellen dürfte. Zum Glück müssen Sie es sich nicht merken. Schließlich geben Sie noch die URL ein und optional ein Verfallsdatum. Wenn Sie auf das Icon neben der URL klicken, dann versucht KeePass, das passende Favicon herunterzuladen. Damit lassen sich Einträge später leichter auffinden.

Falls noch nicht erfolgt, klicken Sie auf das KeePass-Icon in der Symbolleiste des Browsers, um eine Verbindung mit der Passwortdatenbank herzustellen. In KeePassXC selbst können Sie eine URL mit [Strg] + [Umschalt] + [U] direkt im Browser öffnen lassen. Das Programm trägt die Anmeldedaten automatisch ein. Alternativ klicken Sie auf das KeePass-Icon im Eingabefeld.

Wenn Sie eine Webseite besuchen, für die Anmeldedaten in KeePassXC gespeichert sind, werden Sie gefragt, ob Sie den Zugriff zulassen wollen. Dies müssen Sie nur einmal pro Seite bestätigen, indem Sie die Option »Diese Entscheidung merken« aktivieren. Oder Sie deaktivieren diese Sicherheitsfunktion in den Einstellungen. Dazu schalten Sie im Reiter »Fortgeschritten« im Abschnitt »Browser-Integration« die Option »Niemals fragen, bevor auf Anmeldedaten zugegriffen wird« ein.

Gefährlich: Daten exportieren

Ein Export der gesamten in KeePass gespeicherten Daten ist möglich, aber gefährlich: Wenn Sie die Benutzernamen und Passwörter als CSV- oder HTML-Datei abspeichern, werden Ihre sensiblen Informationen anfällig. Wenn Sie es dennoch machen wollen: Der Menüpunkt heißt »Datenbank | Export«.

Recht interessant ist die Statistikfunktion. Sie befindet sich unter »Datenbank | Datenbankeinstellungen«. Wenn Sie in den Bereich »Statistik« wechseln, dann sehen Sie, wie viele Passwörter in KeePass vorliegen, wie viele einzigartig oder gar schwach sind und die durchschnittliche Passwortlänge. Rote Symbole mit weißem X weisen auf Mängel hin.

Log-in-Daten sicher teilen

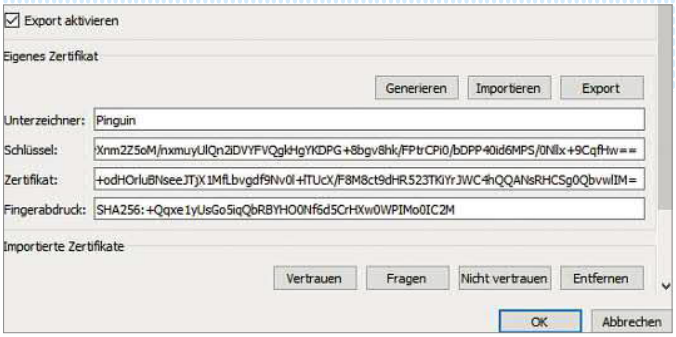
Verwandt mit dem Export ist das Teilen der Daten mit anderen Personen. Die Funktion nennt sich KeeShare. Wenn Ihre Familie Sie nach Ihrem dreißigstelligen Netflix-Passwort fragt, wie übermitteln Sie es? Unverschlüsselte Wege wie E-Mail scheiden aus. Besser geht es mit KeeShare, das zur Synchronisierung von Kennwörtern zwischen mehreren Instanzen von KeePassXC verwendet werden kann. Um die Funktion einzuschalten, gehen Sie zu »Werkzeuge | Einstellungen | KeeShare« und erlauben den Import und Export. Dann erzeugen Sie ein Zertifikat, um Ihre Exportdateien zu signieren, indem Sie auf »Generieren« klicken. Diese Schritte wiederholen Sie für alle beteiligten Datenbanken. KeeShare arbeitet auf Gruppen-Basis, sodass Sie in einer Datenbank mehrere Freigaben für verschiedene Personen einrichten können. Klicken Sie auf »Gruppen | Gruppe bearbeiten« und gehen Sie zum Abschnitt »KeeShare«. Um den Datenfluss zu einer Einbahnstraße zu machen, wählen Sie »Export« in der Masterdatenbank und »Import« in der Zieldatenbank auf dem Rechner des Empfängers aus.

Dann legen Sie Pfad und Passwort fest. Das Passwort ist das gemeinsame Geheimnis zwischen Ihnen und den Empfängern und verschlüsselt die Datei. Sie müssen dieses Kennwort einmal an jede KeePass-Instanz ausliefern. Dazu verwenden Sie

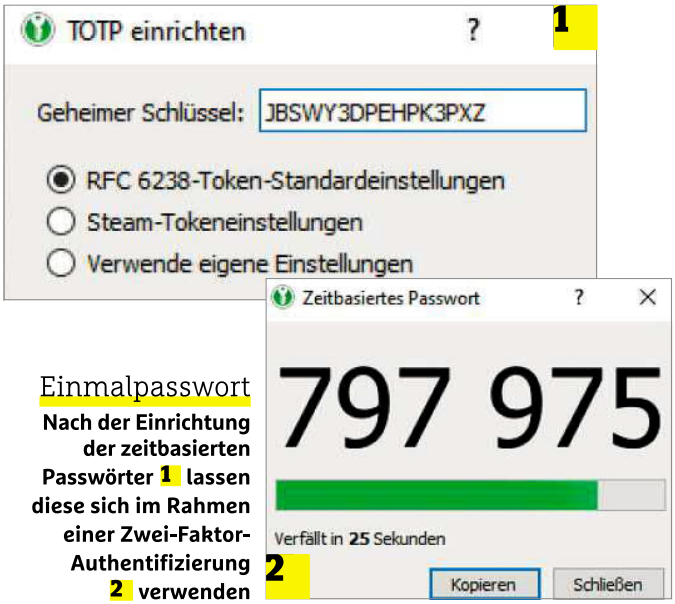
am besten einen sicheren Messenger wie Signal mit selbstzerstörenden Nachrichten. Die Exportdatei wird erst beim Speichern der Datenbank erzeugt.

Zwei-Faktor-Schutz mit KeePassXC nutzen

Die Zwei-Faktor-Authentifizierung (2FA) ist ein wichtiges Sicherheitsfeature vieler Webseiten. Selbst wenn Log-in-Name und Passwort (= 1. Faktor) gestohlen werden, gelangt der Dieb ohne den zweiten Faktor nicht in den Account. Üblich ist heute die Methode »Time-based One-time Password«, kurz TOTP. Sie erzeugt Ziffern aus einem geheimen „Seed" und der aktuellen Zeit, die man zusätzlich zu Log-in und Passwort bei der Anmeldung angeben muss. KeePassXC kann solche TOTP-Seeds für Onlinedienste in einer Datenbank speichern und daraus die entsprechenden zeitgesteuerten Einmalpasswörter generieren. Da 2FA eine getrennte Aufbewahrung von Log-in-Daten und TOTP-Seed erfordert, erstellen Sie in KeePassXC eine separate Datenbank nur für die TOTP-Seeds mit einem eigenen Passwort. Um TOTP zu nutzen, klicken Sie einen Eintrag mit der rechten Maustaste an und wählen »TOTP ... | TOTP einrichten ...«. Geben Sie den Seed an, den Sie von der Webseite erhalten haben, auf der Sie 2FA nutzen wollen. Standardmäßig ist »RFC 6238-Token-Standardeinstellungen« vorausgewählt. Im gleichen Menü lassen Sie sich später mit »TOTP anzeigen ...« das aktuelle Passwort sowie den Countdown bis zur Generierung des nächsten Passworts einblenden. *redaktion@chip.de*



Gruppen lassen sich mit anderen KeePassXC-Instanzen teilen. Die exportierte Datei kann mit einem Zertifikat signiert werden



Einmalpasswort

Nach der Einrichtung der zeitbasierten Passwörter 1 lassen diese sich im Rahmen einer Zwei-Faktor-Authentifizierung 2 verwenden

SHORTCUT

Der Inhalt in 30 Sekunden

Passwörter sollen lang sein und für jeden Dienst individuell vergeben werden. Dabei hilft der Passwortmanager KeePassXC, der Log-in-Daten speichert und diese über Browser-Plug-ins und eine Android-App über verschiedene Geräte und unterschiedliche Browser verfügbar macht. KeePass kann auch 2FA-Codes erzeugen.

Sync mit dem Smartphone

Um auch auf Android-Geräten von dem Passwortmanager profitieren zu können, legen Sie den Passortcontainer in einen Cloudspeicher wie Dropbox, OneDrive oder Google Drive.

> **Das ist unbedenklich,** da der Datentresor sicher verschlüsselt und daher für den Cloudbetreiber nicht einsehbar ist. Sie erkennen ihn an der Datei-Endung »kdbx«. Als Apps benötigen Sie einen Cloudspeicher wie Google Drive und Keepass2Android. Beides finden Sie im Google Play Store. Die App unterstützt Dropbox, Google Drive, OneDrive, Owncloud, FTP und WebDAV.

> **Legen Sie den Container** in der Cloud ab. Nach dem Start vergeben Sie in Keepass2Android die nötigen Berechtigungen und laden die Containerdatei aus dem Cloudspeicher. Das praktische Feature »QuickUnlock« erleichtert die Eingabe des hoffentlich komplizierten Passworts. Ist die Option aktiviert, genügt die Eingabe der letzten drei Zeichen. Nach Ablauf eines voreingestellten Zeitraums, einem falschen Log-in-Versuch oder dem Beenden von Programm oder Android selbst muss wieder das vollständige Passwort eingegeben werden. Damit bietet QuickUnlock einen guten Kompromiss aus Sicherheit und Komfort. Auch eine Freigabe per Fingerabdruck ist möglich.

> **Keepass2Android** funktioniert ähnlich wie die PC-Version. Die App läuft ständig im Hintergrund und achtet auf Log-in-Felder. Wenn Sie auf dem Smartphone eine App öffnen, halten Sie den Finger kurz auf dem Eingabefeld gedrückt. Dann erscheint ein Keepass-Pop-up mit den Zugangsdaten. Da Keepass2Android eine eigene Tastatur mitbringt, lässt sich das potenziell unsichere Einfügen über die Zwischenablage umgehen. Für iOS existiert eine ähnliche App namens Strongbox.

Die App Keepass2Android kann Passwortcontainer von KeePassXC öffnen. Zum Übertragen bietet sich ein Cloudspeicher an