



Schlüsselfertig

So bringen Sie Ordnung ins Passwort-Chaos

Passwörter sollten möglichst lang und kompliziert sein, zudem sollte man sie jeweils nur für einen Dienst verwenden – Anforderungen, die es nicht gerade leicht machen, sich alle benutzten Kennwörter zu merken. Der Passwort-Manager KeePass nimmt Ihnen die Gedächtnisarbeit ab und verwahrt Ihre Geheimnisse sicher. Mit unseren Tipps ist die Einrichtung gar nicht so schwer.

Von Marvin Strathmann

Für den alten Windows-Rechner hatte ich mir doch mal ein besonders kniffliges Passwort ausgedacht – aber endete das mit [S0 oder mit {50? Opa Günthers Passwörter stehen auf einem Post-it am Rand des Monitors; er benutzt für alle Webseiten dasselbe. Das WLAN-Passwort der WG klebt unter dem Router, aber wo stand eigentlich das Kennwort für das Kundenportal des Providers? Und mit welcher E-Mail sind wir da angemeldet?

Es ist gar nicht so einfach, im Passwort-Chaos den Durchblick zu behalten. Man ist bei Dutzenden Diensten angemeldet, die ein sicheres Kennwort verlangen – Groß- und Kleinbuchstaben, Ziffern,

Sonderzeichen. Gleichzeitig sollte man für jeden Dienst ein anderes Passwort verwenden. Diese Regeln machen Passwörter sicher, aber verwirren den Menschen: Keiner behält all diese Daten im Kopf.

Die gute Nachricht: Sie können Ordnung in diesen vermeintlich unbeherrschbaren Wust aus Passwörtern bringen – unsere Anleitung zeigt, wie. Als Resultat liegt eine Datenbank auf Ihrem Rechner, in der Sie Ihre Passwörter übersichtlich und sicher verwalten. Alle Passwörter sind verschieden, so können Sie schnell reagieren, wenn Kriminelle mal wieder Passwörter eines Unternehmens erbeuten. Dank Erweiterungen für den Browser werden viele

Anmeldefelder automatisch ausgefüllt, Sie sparen sich lästige Tipparbeit. Über ein Backup sind Sie gegen Datenverlust abgesichert.

Als Werkzeug verwenden wir den Passwort-Manager KeePass. Wegen der großen Verbreitung beschreiben wir seinen Einsatz auf Windows 10. Als Browser dient im Beispiel Firefox. Sie wollen einen anderen Manager verwenden, besitzen einen Mac und Ihr Lieblings-Browser ist Chrome? Kein Problem, andere Programme und Systeme arbeiten in der Regel ähnlich. Daher lässt sich diese Anleitung leicht als Blaupause für andere Szenarien verwenden. Ein bisschen Zeit sollten Sie allerdings einplanen – Sie werden mehrere Stunden benötigen.

Ärmel hoch

KeePass ist kostenlos, Open Source und bietet viele Erweiterungen. Das Programm speichert die Kennwörter standardmäßig nicht in der Cloud, sodass Sie stets die komplette Kontrolle über Ihre Daten haben.

Auf der Webseite des Projekts können Sie KeePass für Windows herunterladen (für alle Downloads siehe ct.de/yqbt). Oben links finden Sie die aktuelle 2.x-Version der Software, die wir für diese Anleitung verwenden, konkret Version 2.41. Ein Klick auf den grünen Button startet den Download.

Falls Sie KeePass 2.x auf einem USB-Stick installieren und immer dabei haben wollen, wählen Sie die portable Version rechts daneben. Unterhalb der beiden Optionen finden Sie Download-Links für die 1.x-Version von KeePass. Sie wird parallel zur 2.x-Version entwickelt und kommt ohne das .NET Framework von Microsoft aus. Daher bietet sie weniger Funktionen als die 2.x-Version (Details über ct.de/yqbt). Auf der Projekt-Seite finden Sie zudem Anleitungen, wie Sie KeePass 2.x unter macOS und Linux zum Laufen kriegen.

Das Programm selbst ist komplett in Englisch gehalten. Das lässt sich ändern: Auf der Projekt-Seite des Programms finden Sie Sprachdateien als Download. Laden Sie die deutsche ZIP-Datei für Version 2.x herunter und entpacken Sie die Datei German.lngx in den Languages-Ordner im KeePass-Verzeichnis. Wenn Sie bei der Installation die Vorgaben beibehalten haben, finden Sie den Ordner unter „C:\Program Files (x86)\KeePass Password Safe 2\Languages“. Zurück in Kee-

Pass klicken Sie auf „View“, dann auf „Change Language“ und wählen unter „Installed Languages“ den Eintrag „German (Deutsch)“ aus. Anschließend starten Sie KeePass neu.

Passwort-Datenbank anlegen

Weiter geht es mit der Passwort-Datenbank: Klicken Sie auf „Datei“, anschließend auf „Neu“ und bestätigen Sie den aufpoppenden Hinweis. Wählen Sie einen gut zu merkenden Speicherort für Ihre Passwort-Datenbank.

Nun fordert KeePass Sie auf, einen Hauptschlüssel zu wählen. Jedes Mal, wenn Sie die Passwort-Datenbank öffnen, müssen Sie ihn eingeben. Dieser Hauptschlüssel wird das wichtigste Passwort, das Sie in Zukunft verwenden werden. Mit ihm greifen Sie auf die gesamte Passwort-Datenbank zu, er ist wie ein General-schlüssel für all Ihre Accounts. Deshalb gilt: Sie müssen sich den Hauptschlüssel gut merken können, gleichzeitig soll er besonders sicher sein.

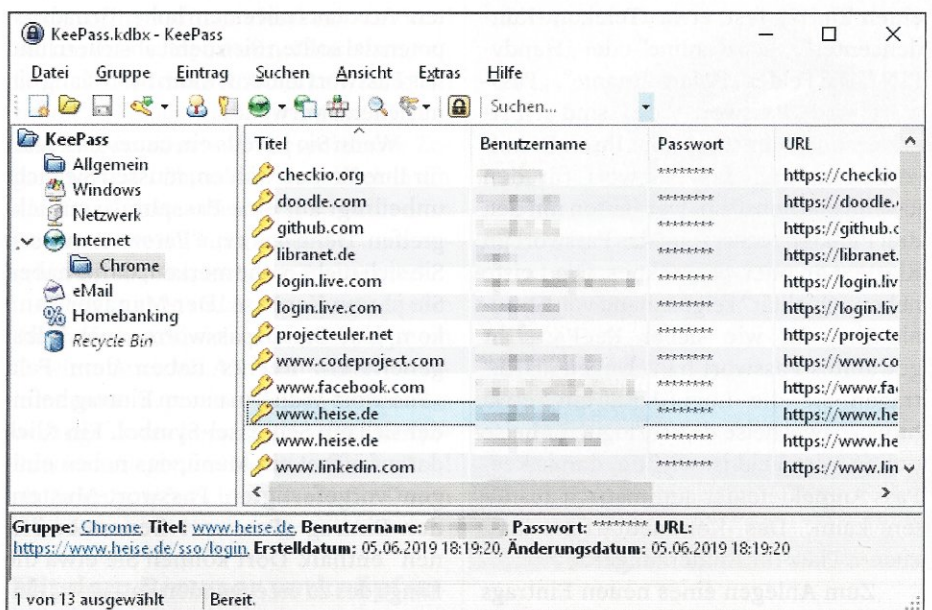
Eine Passphrase erfüllt diese Voraussetzungen: Das kann etwa ein kompletter Satz oder können zufällige Wörter hintereinander sein. Die Phrase ist leichter zu merken als ein Gemenge aus Sonderzeichen und mit ihrer Länge so komplex, dass man sie durch Ausprobieren kaum erraten kann. Falls Ihnen gerade kein für Sie einfach zu merkender, aber für Fremde schwer zu erratender Satz einfällt, können Sie auch einfach zufällige Wörter zu einer

Phrase kombinieren. Dazu schlagen Sie beispielsweise ein Buch auf zufälligen Seiten auf und tippen mit geschlossenen Augen auf zufällige Stellen. Wörterbücher oder Lexika bieten sich hier besonders an, aber auch ein Harry Potter leistet gute Dienste. Wiederholen Sie den Vorgang drei oder vier Mal, schon haben Sie eine Passphrase kreiert, die keiner erraten kann.

Wer gerade kein Buch zur Hand hat, kann auf eine deutsche Diceware-Liste aus dem Netz zurückgreifen, benötigt aber einen Würfel (Englisch: Dice). Sie würfeln fünf Mal und notieren jeweils die Augenzahl: In dem unter ct.de/yqbt verlinkten Beispiel würde die Abfolge 5, 3, 1, 1, 2 „rocker“ ergeben. Auch das wiederholen Sie mindestens drei Mal und setzen so Ihre Phrase zusammen.

Ob Sie die Wörter mit einem Leerzeichen trennen oder jedes Wort mit einem Großbuchstaben beginnen, bleibt Ihnen überlassen. Auch ein Sonderzeichen am Ende kann nicht schaden, aber Ihre Passphrase ist auch so schon sehr komplex und unberechenbar.

Tragen Sie Ihre Phrase neben „Hauptpasswort“ in KeePass ein und wiederholen Sie die Eingabe darunter. Phrasen, die mehr als 128 Bit Informationsgehalt (Entropie) aufweisen, stuft KeePass als sehr sicher ein. Wenn Sie die Expertoptionen einschalten, können Sie mit einer zusätzlichen Schlüsseldatei arbeiten oder den aktuellen Benutzer-Account von Windows verknüpfen.



Das Hauptfenster von KeePass unterteilt sich in drei Teile: links der Ordnerbaum, rechts das Eintrags-Feld und unten das Informations-Feld.

Nun geben Sie der Datenbank einen internen Namen. Der Einfachheit halber können Sie die Datenbank so nennen wie die dazugehörige Datei. Die restlichen Einstellungen belassen Sie so, wie sie sind.

Zuletzt empfiehlt KeePass, ein Notfallblatt auszudrucken, wo etwa der Speicherort der Datenbank-Datei zu finden ist und Sie den Hauptschlüssel eintragen können. Auch wenn Sie das Blatt nicht ausdrucken: Es ist sinnvoll, die Passphrase aufzuschreiben und sicher zu verwahren, optimal in einem Tresor.

Passwort-Einträge hinzufügen

Ihre Datenbank ist nun startklar. Das Hauptfenster von KeePass ist in drei Teile gegliedert. In der Ordnerstruktur links organisieren Sie Ihre Passwort-Einträge. KeePass hat bereits einige Ordner erstellt, etwa „Netzwerk“, „eMail“ oder „Allgemein“. Wenn Sie auf einen Ordner klicken, zeigt KeePass rechts die Einträge im Ordner an. Zwei Beispiele liefert das Programm gleich mit. Im Root-Ordner, der so heißt wie Ihre Datenbank, finden Sie die Einträge „Beispieleintrag“ und „Beispieleintrag #2“ mit fiktiven Daten und schlecht gewählten Passwörtern. Wenn Sie einen Eintrag auswählen, erhalten sie unten weitere Informationen, etwa das Erstelldatum oder eingetragene Kommentare. Nach einem Rechtsklick können Sie beispielsweise Passwort oder Benutzername kopieren.

Per Doppelklick auf einen Eintrag bearbeiten Sie die Daten. Im Feld „Titel“ legen Sie einen eindeutigen Namen für einen Eintrag fest, etwa „Telekom-Kundencenter“, „heise online“ oder „Handy-PIN“. Die Felder „Benutzername“, „Passwort“ und „Passwort-Wdh.“ sind selbst erklärend – hier tragen Sie Ihren Benutzernamen und das Passwort für den jeweiligen Dienst ein. Der Button mit den drei Punkten rechts zeigt das Passwort im Klartext an oder versteckt es. Die Leiste neben „Qualität“ zeigt anhand von Entropie-Bits, für wie sicher KeePass Ihr gewähltes Passwort hält. Neben „URL“ tragen Sie die Login-URL ein, etwa <https://www.heise.de/sso/login> für heise online – das Feld ist wichtig, damit KeePass Anmeldefelder automatisch ausfüllen kann. Das Kommentarfeld lässt zudem Platz für Anmerkungen.

Zum Anlegen eines neuen Eintrags klicken Sie auf den Schlüssel mit dem kleinen grünen Pfeil in der Symbolleiste. Alternativ wählen Sie den Menübefehl „Ein-

trag/Eintrag hinzufügen“ oder drücken Strg+I.

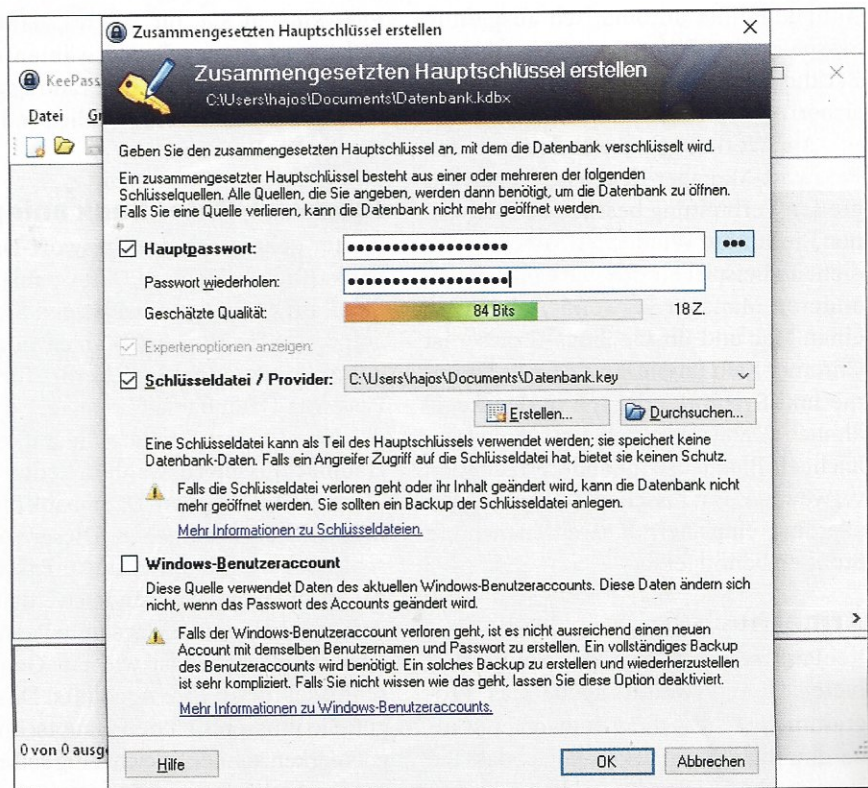
Jetzt beginnen Sie damit, Ihren Passwort-Berg abzutragen, und erstellen pro Account einen neuen Eintrag. Starten Sie mit Ihren wichtigsten Konten. Eine Frage hilft bei der Auswahl: Wenn Kriminelle Zugriff auf dieses Konto hätten, wie groß wäre der Schaden, den sie anrichten könnten? Accounts mit einem hohen Schadenspotenzial sollten Sie zuerst absichern und das Passwort ändern, wenn Sie bislang ein unsicheres verwenden.

Wenn Sie jeweils ein neues Passwort für Ihre Konten wählen, müssen Sie nicht unbedingt auf eine Passphrase zurückgreifen. Denn das neue Passwort müssen Sie sich nicht mehr merken, dafür haben Sie ja nun KeePass. Der Manager kann komplexe Zufallspasswörter auch selbst generieren: Rechts neben dem Feld „Passwort-Wdh.“ in einem Eintrag befindet sich ein Schlüssel-Symbol. Ein Klick darauf öffnet ein Menü, das neben einigen vorgefertigten Passwort-Mustern den Eintrag „Passwort-Generator öffnen“ enthält. Dort können Sie etwa die Länge des zu erzeugenden Passworts einstellen oder Sonder- und weitere Zeichen integrieren. Über das Disketten-Symbol oben rechts können Sie ihre Auswahl

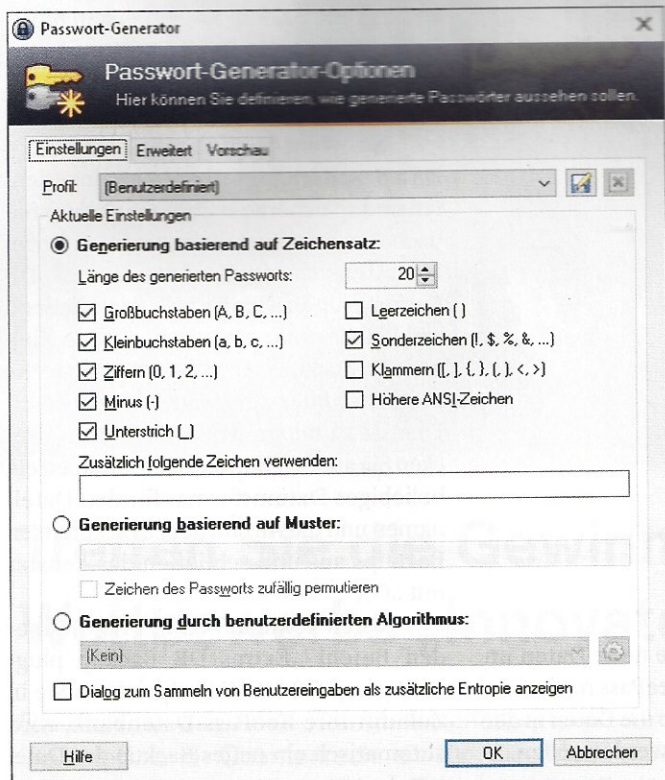
speichern und anschließend schneller darauf zugreifen.

Passwörter zu ändern dauert. Denn Sie können so viel in KeePass eintragen, wie Sie möchten, das Passwort des Kontos haben Sie damit nicht geändert. Dafür müssen Sie sich erst bei den Diensten mit Ihren bisherigen Daten einloggen, die Sicherheits- oder Kontoeinstellungen finden, ein neues Passwort eintragen und im Anschluss meist diverse E-Mails bestätigen. Jeder Dienst geht unterschiedlich vor. Speichern Sie den KeePass-Eintrag erst mit „OK“, wenn Ihr Dienst das neue Passwort akzeptiert hat – Dienst und KeePass sind nun auf demselben Stand.

Speichern Sie Ihre Datenbank zwischendurch immer wieder ab. In der Symbolleiste des Hauptfensters klicken Sie dazu das blaue Diskettensymbol oder drücken Strg+S. Ein automatisches Speichern ist von Haus aus nicht aktiviert, aber über das Menü „Optionen“, den Reiter „Erweitert“ und einen Haken neben „Automatisch speichern, nachdem ein Eintrag mit dem Eintrag-Bearbeitungsdialog geändert wurde“ holen Sie das nach. Ein Haken neben dem darüber liegenden „Automatisch speichern, wenn die Datenbank geschlossen/gesperrt wird“ kann ebenfalls nicht schaden.



Der Hauptschlüssel wird das wichtigste Passwort, das Sie in Zukunft verwenden.



Mit dem Passwort-Generator können Sie über komplexe Regeln Zufalls-kennwörter erzeugen.

Nachdem Sie Ihre wichtigsten Accounts geändert und in die Datenbank eingetragen haben, steht es um Ihre Passwort-Sicherheit schon sehr viel besser. Wenn Sie neue Accounts hinzufügen, sollten sie sich angewöhnen, gleich einen Eintrag in KeePass anzulegen und sich ein sicheres Passwort generieren zu lassen.

Weitere Accounts

Um die Passwörter sämtlicher Dienste zu ändern, bei denen Sie angemeldet sind, müssen Sie sie erst einmal finden – im Laufe der Zeit vergisst man gerne, wo man überall ein Konto hat. Startpunkt bildet Ihre E-Mail, denn im Postfach wimmelt es wahrscheinlich nur so von Willkommens-Mails, Newslettern oder Änderungen der Nutzungsbedingungen.

Hier ist ein wenig Detektivarbeit gefragt. Suchen Sie nach Standardfloskeln in Anmelde-Mails wie „Willkommen“, „Zugangsdaten“ oder „Registrierung“, gerne auch auf Englisch. Wegen der DSGVO haben im Mai 2018 viele Unternehmen ihre Datenschutzerklärung geändert und ihre Nutzer benachrichtigt; „Datenschutzrichtlinie“, „Datenschutzerklärung“ oder „Nutzungsbedingungen“ sind daher vielversprechende Suchbegriffe. Zusätzlich können Sie nach „Newsletter“ oder „Unsubscribe“ suchen und damit Dienste anzeigen lassen, die Ihnen einen

Newsletter schicken. Für jede Fundstelle melden Sie sich beim dazugehörigen Dienst an und ändern das Passwort – Eintrag in KeePass nicht vergessen. Falls Sie den Account nicht mehr benötigen, melden Sie sich gleich von dem Dienst ab – auch Datensparsamkeit erhöht die Sicherheit.

Auch die Passwort-Speicher von Browsern können zeigen, wo Sie überall angemeldet sind. Bei Firefox klicken Sie oben rechts auf das Menü mit den drei Balken und wählen dann „Einstellungen“, links „Datenschutz & Sicherheit“, scrollen runter zu „Zugangsdaten & Passwörter“ und klicken dann auf „Gespeicherte Zugangsdaten“. Chrome-Nutzer klicken auf die drei Punkte oben rechts, wählen im Reiter „AutoFill“ „Passwörter“ und anschließend „Gespeicherte Passwörter“.

Jedes alte Standard-Passwort, das Sie durch ein neues, sicheres ersetzen, ist ein Gewinn. Auch WLAN-Kennwörter, Telefonnummern, private Notizen und andere wichtige Daten können Sie sicher in KeePass hinterlegen – betrachten Sie das Tool als Ihren persönlichen Tresor für Daten aller Art.

Mit dem Browser verknüpfen

KeePass kann Passwörter nicht nur sicher speichern, sondern auch den Umgang damit sehr komfortabel machen. Auf der

Smarte Gadgets

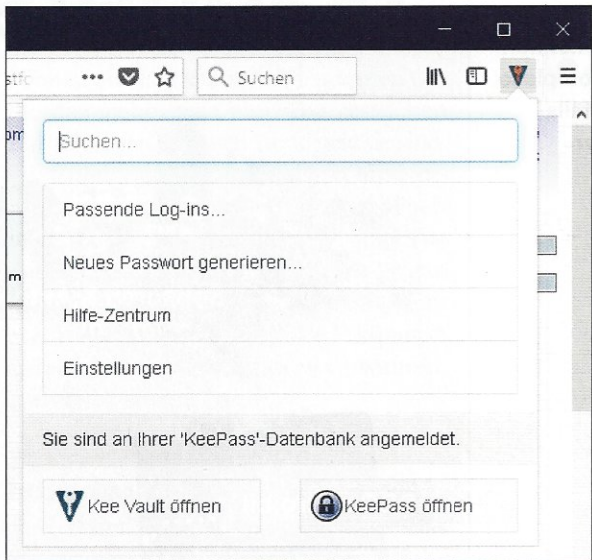


PORTOFREI
AB 15 €
BESTELLWERT

Bestellen Sie ganz einfach online unter shop.heise.de
oder per E-Mail: service@shop.heise.de

 **heise shop**

shop.heise.de/hardware



Mit der Browser-Erweiterung Kee können Sie Ihre Passwort-Datenbank im Browser durchsuchen.

Programm-Website sind dazu Dutzende Plug-ins gelistet. Alle Erweiterungen, die mit dem blauen Label „2.x“ versehen sind, funktionieren mit der hier vorgestellten Version des Programms.

Auf der Seite finden Sie unter anderem das Plug-in Kee, das KeePass mit dem Webbrowser verbindet. Es füllt automatisch Formulare aus und spart Ihnen so lästige Tipp- oder Copy&Paste-Arbeit. Dafür laden Sie zunächst das Plug-in KeePassRPC herunter und verschieben die .plgz-Datei in den Plugins-Ordner des KeePass-Verzeichnisses. Ein Neustart von KeePass aktiviert das Plug-in. Anschließend installieren Sie das Add-on Kee für Firefox oder Chrome.

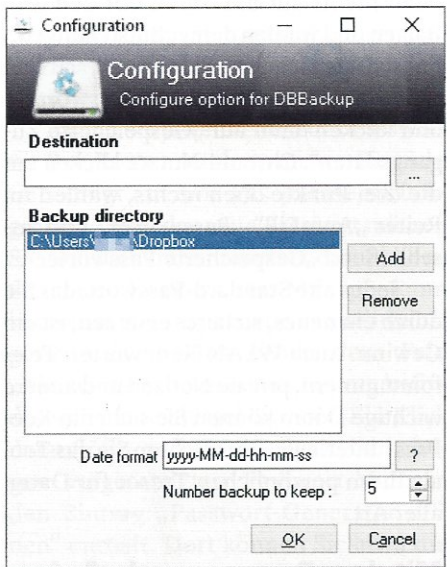
Kee fragt nach einem Autorisierungspasswort, das Sie in einem neu geöffneten KeePass-Fenster finden. Kopieren Sie die sechs roten Zeichen und fügen Sie sie in das Passwort-Feld der Kee-Erweiterung im Browser ein. Auf „Verbinden“ drücken, fertig.

Wenn Sie fleißig die jeweiligen Login-URLs in Einträgen vermerkt haben, erkennt Kee den passenden Eintrag und füllt das Anmeldeformular automatisch aus. Das klappt aber nicht immer: Über das neue dreieckige Symbol in der Symbolleiste können Sie Kee nach den richtigen Einträgen suchen lassen oder die Datenbank per Hand durchforsten. Zudem zeigt das Plug-in das dreieckige Symbol in den Formularfeldern an. Wenn Sie dort draufklicken, können Sie passende Login-Daten auswählen, falls Kee danebenliegt oder es mehrere Möglichkeiten gibt, etwa weil Sie bei einem Dienst mehrere Konten haben.

Praktisch: Wenn Sie neue Daten im Browser eingeben, die KeePass noch nicht kennt, dann fragt Kee, ob die Daten in der Datenbank gespeichert werden sollen.

Backup

KeePass und die Datenbankdatei mit Ihren Passwörtern werden schnell zu einem täglichen Begleiter auf Ihrem Desktop. Geht die .kdbx-Datei aber verloren, war all Ihre Arbeit umsonst und sämtliche Kennwörter sind weg. Sie müssten über die jeweiligen Passwort-Vergessen-Funktionen der Dienste Ihre Kennwörter zurücksetzen und neue anfordern – ein ziemlicher Aufwand. Legen Sie daher un-



Das Plug-in DataBaseBackup besitzt eine übersichtliche Konfiguration und speichert zuverlässig.

bedingt ein Backup an, um gegen plötzliche Hardwaretode, Brände und verpfuschte Updates von Microsoft abgesichert zu sein.

Dabei hilft beispielsweise das Plug-in DataBaseBackup. Es ist leicht einzurichten und speichert die Datenbank automatisch. Nach der Installation wählen Sie im Hauptfenster von KeePass „Extras/DB Backup plug-in/Configure“. Anschließend wählen Sie unter „Destination“ den Zielort des Backups: Ein NAS, eine externe Festplatte oder der Ordner eines Cloud-Dienstes sind sinnvolle Ziele. Nun drücken Sie auf den Button „Add“, wählen ein beliebiges Datumsformat für den Dateinamen und die Anzahl der zu behaltenden Backups aus und schließen das Fenster mit „OK“.

Testen können Sie das Plug-in über den Befehl „Extras/DB Backup plug-in/Backup DB NOW !“. Speichern Sie in Zukunft Ihre KeePass-Datenbank, wird automatisch ein neues Backup der Datei angelegt.

Falls Sie kein Plug-in installieren wollen, können Sie ein automatisches Backup auch mit der eingebauten Trigger-Funktion einrichten. Auf der KeePass-Website finden Sie dazu eine ausführliche Anleitung.

Als externes Backup-Tool können Sie beispielsweise das kostenlose Programm Duplicati ausprobieren [1]. Falls Sie amerikanischen Cloud-Anbietern Ihre Datenbank-Datei nicht anvertrauen möchten, können Sie eine private Cloud auf Ihrem eigenen Server einrichten [2].

Mit dem Passwort-Manager KeePass ist noch sehr viel mehr möglich. Über diverse Apps können Sie beispielsweise Ihre Datenbank auf dem Android-Smartphone verwenden [3]. Mit KeePass können Sie zudem Einmalpasswörter generieren und das Programm damit für die Zwei-Faktor-Authentifizierung einsetzen [4].

(hos@ct.de) ct

Literatur

[1] Ronald Eikenberg, Backups vom Fließband, Mit Duplicati in fünf Minuten zum Trojaner-sicheren Backup, c't 11/2016, S. 108
[2] Jan Mahn, Synchrone Satelliten, Vier Programme für Peer-to-Peer-Synchronisation im Test, c't 23/2018, S. 78
[3] Stefan Porteck, Datenschieber, Passwörter mit KeePass unter Android verwalten, c't 8/2018, S. 144
[4] Merlin Schumacher, Doppelt hält besser, Bequeme Zwei-Faktor-Authentifizierung mit KeePass, c't 22/2018, S. 172

KeePass, weitere Tools, Dokumentationen: ct.de/yqbt