Logins mitnehmen

Keepass-Passwörter unter iOS verwalten

Der Passwortmanager Schlüsselbund von Apple versteht sich nicht mit Keepass. Was also tun, wenn zu Hause ein Windows-Rechner mit eben diesem Programm seinen Dienst tut? Mit Keepassium und Strongbox kommen Sie auch mit iOS an Ihre in Keepass gespeicherten Daten heran.

Von Marvin Strathmann

wer Passwörter und andere Zugangsdaten mit einem Tool verwaltet, möchte sie in der Regel auch mobil dabeihaben. Die Kennwortdatenbank bringt ja nichts, wenn sie auf dem Desktoprechner liegt, man aber auf dem Smart-TV des Freundes seine Netflix-Zugangsdaten eingeben möchte und nur sein iOS-Gerät dabei hat.

Die Kennwörter müssen also aufs Handy. Wer bereits den beliebten Passwortmanager Keepass verwendet, muss dafür auf einen Ableger zurückgreifen. Auch die Apps, die auf Keepass aufsetzen verzichten auf eine eigene Cloud-Anbindung, sodass der Nutzer die volle Kontrolle behält, wo er seine Passwortdatenbank speichert. Offiziell gibt es Keepass nämlich nur für den Windows-Desktop. Doch die Community für den kostenlosen Open-Source-Manager ist groß. Gleich mehrere iOS-Apps können mit dem KDBX-Format von Keepass umgehen.

App-Auswahl

Auf den ersten Blick gibt es sehr viele Keepass-Umsetzungen für iOS. Die offizielle Keepass-Seite listet insgesamt acht inoffizielle Portierungen für das iPhone beziehungsweise das iPad (siehe ct.de/y4ad). Viele Apps auf der Liste sind hoffnungslos veraltet, etwa Synchpass, Passwordix, iKeepass oder Passdrop 2. Die auf der Keepass-Seite aufgeführte App Mykeepass ist sogar vollständig aus dem App Store verschwunden, letzte Aktivitäten gab es anscheinend 2010.

Keepass Touch ist relativ neu und steht nicht auf der offiziellen Liste des Entwicklers. Die App fußt auf dem beliebten Minikeepass für iOS, das 2020 eingestellt wurde. Ein offizielles Repository gibt es für Keepass Touch nicht. Zusätzlich hält sich die App nicht an die Namenskonvention, die Keepass-Entworder Derman Reichl vorgegeben hat. Derman "Keepass" im Namen des Aller alleine stehen – Keepassdood der Teepassium sind okay, Keepass Touch der Tee-Aus diesen Gründen lassen die Tee-Touch hier außen vor.

Dieser Artikel behandet messen aktuelle Apps. Beide gibt es also and an and a series and a serie

Keepassium

Keepassium installieren Sie wie gewohnt über den App Store (siehe ct.de/y4ad). Beim ersten Start fragt die App, ob Sie eine neue Datenbank erstellen oder eine vorhandene Datenbank hinzufügen möchten. Sollten Sie keine Keepass-Datenbank

besitzen, tippen Sie auf "Neue Datenbank erstellen". Vergeben Sie einen Namen, zum Beispiel "Passwörter" oder schlicht "Datenbank". Anschließend verlangt die App den Hauptschlüssel für die Datenbank. Das ist das sozusagen der Generalschlüssel – über diesen greifen Sie in Zukunft auf alle anderen Passwörter in der App zu. Der Hauptschlüssel sollte lang, aber gut zu merken sein. Mehrere zufällig ausgewählte Wörter aus einem Buch oder einer Liste erfüllen diesen Zweck. Falls Sie eine bereits vorhandene Datenbank hinzufügen, verwenden Sie den dafür angelegten Hauptschlüssel, um sie zu entsperren.

Zusätzlich zu diesem Kennwort können Sie optional eine Schlüsseldatei anlegen. Dieser zweite Faktor erhöht die Sicherheit. Wenn Sie eine Schlüsseldatei erstellen, sollten Sie diese lokal lagern, und zwar nicht mit der Passwortdatenbank zusammen. Nur wer das Hauptpasswort kennt und die Schlüsseldatei besitzt, kann auf die Passwörter zugreifen. Neben dem Schlüsseldatei-Feld finden Sie noch ein blaues USB-Stick-Symbol. Hier können Sie in der Premiumversion einen Yubikev als Hardwaretoken statt eines Passworts oder einer Schlüsseldatei festlegen. Keepassium verschlüsselt mit Argon2 und Chacha20 und kann mit der aktuellen Version 4.1 des KDBX-Formats umgehen.

Anschließend lässt sich die Datenbank etwa auf dem Gerät speichern oder bei einem installierten Synchronisierungsdienst wie Dropbox, iCloud Drive oder Google Drive ablegen. Ist ein Dienst ausgegraut und die Datei dort nicht speicherbar, reicht es meist aus, den Dienst in der Dateien-App von Apple als Speicherort zu aktivieren.

Neue Einträge erstellen

Über das blaue Plussymbol neben dem Namen der Datenbank können Sie einen Ordner oder neuen Eintrag hinzufügen. Keepassium bezeichnet Ordner als Gruppen und bringt bereits sechs Vorschläge mit. Bezeichnung, Reihenfolge und Symbol lassen sich beliebig ändern. Alternativ löschen Sie Ordner und legen eigene an.

In der Eingabemaske für neue Passworteinträge geben Sie zunächst eine Bezeichnung ein, etwa "Google Mail". Anschließend füllen Sie alle Felder aus. Sofern Sie immer wieder denselben Nutzernamen verwenden, müssen Sie diesen nicht jedes Mal erneut eingeben. Stattdessen tippen Sie auf "Auswählen". Die App blendet eine Liste mit bereits verwendeten Einträgen ein. Außerdem schlägt Keepassium drei Zufallsnamen vor, die immer wieder variieren.

Neue Passwörter müssen Sie sich künftig nicht mehr selbst ausdenken. Die App bringt einen Zufallsgenerator mit: Darin stellen Sie die Länge des Passworts ein und wählen aus, ob es Symbole oder Ziffern enthalten soll. Über das Pfeilsymbol oben rechts generiert Keepassium einen neuen Vorschlag, falls der alte nicht gefällt. Achten Sie darauf, dass hinter der Option "Ähnlich aussehende Zeichen" kein Häkchen gesetzt ist. So verhindern Sie Verwechslungen bei Zeichen wie 1, I und I oder O und 0.

Carterionimetr	Ale 13	and the set of the	wakommen	Part and
nne Datenbank	Abbrechen	Neue Datenbank er	rstellen	- E
Sie KeePassium v Igten Zugriffen.				
opsperre aktiviere		Name der Datenbank		recitkarten
		MyPasswords		Pusseken
		Hauptschlüssel		1 um zum
		Passwort	۲	ionten zu
		Rome Schildstel	0	1 million
		Datenbark speichen	n unter	
		kaloof Facenat vervee (Anpar0+ChaChaD	cultern 106	100 L
				1
				A Mandala
				Res and

Um eine Datenbank in Keepassium anzulegen, müssen Sie nur wenige Felder ausfüllen.

Die Eingabemaske lässt sich durch eigene Felder ergänzen, indem Sie auf das Plussymbol oben rechts tippen. Titel und Inhalt dieser Felder sind anschließend frei wählbar. Das kann etwa ein Feld für die Sicherheitsfrage samt Antwort sein, die manche Anbieter zusätzlich zum Passwort abfragen.

Außerdem lässt sich noch das Symbol des Eintrags ändern. Standardmäßig ist das ein blauer Schlüssel. Keepassium bringt noch mehr als 60 weitere Symbole in einem ähnlichen Stil mit. Alternativ verwenden Sie eigene Fotos oder Symbole.

One-Time-Password hinzufügen

Schließlich lässt sich unten noch ein One-Time-Password (OTP) für den Eintrag festlegen. Ein OTP ist ein zweiter Faktor, der zusätzlich zu dem normalen Passwort eingegeben werden muss. Das OTP ist vergleichbar mit einer TAN, die ein eingeloggter Nutzer beim Onlinebanking

< Schließe	en 🛅 MyPasswords	+	P Beispieleintrag Bearbeiten
Allg	jemein	0 >	Allgemein Dateien Verlauf
Inte	ernet	0 >	Benutzername john.smith
Ema	ail	0 >	Passwort
Sc Fina	anzen	0 >	****
Net	zwerk	0 >	URL Cr https://keepassium.com C
💍 Bet	riebssystem	0 >	Kommentare
P Beis	spieleintrag smith		Sie können auch einige Notizen speichern, wenn Sie möchten.

Anhand des Beispieleintrags können sich Einsteiger einen Überblick über die Möglichkeiten der Einträge verschaffen. stellen.



eingeben muss, um eine Aktion zu bestätigen.

Um diese Funktion zu nutzen, müssen Sie sie vorher beim Anbieter aktivieren-vor allem große Dienste bieten das an, etwa Gmail, Dropbox und Evernote. Der Anbieter spuckt einmalig einen QR-Code aus, den Sie mit Keepassium scannen. Die App erstellt nun ein neues Feld namens OTP und legt eine URL im Format "otpauth://..." darin ab. Danach zeigt die App das ständig wechselnde Passwort an, das bei einem Zwei-Faktor-Login benötigt wird. Ein kleiner blauer Balken unter dem Code deutet an, wie lange er noch gültig ist.

Datenbank sortieren und sperren

Auf der Übersichtsseite finden Sie unten links Sie vier Symbole. Über das erste mit den Strichen und dem Pfeil legen Sie fest, wie die App Einträge sortieren soll. Außerdem lässt sich der Untertitel festlegen, der unter jedem Eintrag erscheint - zunächst ist das der Benutzername, aber auch Klartextpasswort und das letzte Bearbeitungsdatum sind möglich.

Das Schlosssymbol sperrt die Datenbank. Über das Schlüsselsymbol mit dem kleinen Schild ändern Sie den Hauptschlüssel der Datenbank oder legen nachträglich noch eine Schlüsseldatei fest. Ein Tipp auf das Zahnradsymbol rechts in der Leiste öffnet die allgemeinen App-Einstellungen.

Einstellungen

Damit Keepassium die Autofill-Funktion nutzt, gehen Sie zunächst in die Einstellungen ihres iOS-Gerätes. Unter "Passwörter" beziehungsweise "Passwörter & Accounts" finden Sie die Option "Automatisch ausfüllen". Dort legen Sie Keepassium als Standard fest. In den Einstellungen von Keepassium finden Sie die Option im Eintrag "Passwörter automatisch eintragen". Hier lässt sich auch festlegen, ob Keepassium ein OTP automatisch in die Zwischenablage packen soll.

Um Keepassium künftig per Fingerabdruck zu entsperren, tippen Sie auf "Zugangsschutz" und aktivieren "Touch ID verwenden". Auch die Einstellungen für Face ID finden Sie an dieser Stelle, wenn Ihr Gerät diese Funktion anbietet. Zusätzlich lässt sich hier eine PIN für die App eintragen und eine Wartezeit festlegen, nach der Keepassium automatisch gesperrt wird und Sie sich erneut einloggen müssen.

Backup

Keepassium legt vor dem Speichern einer Datenbank stets ein Backup an. Sie können Sicherungen aus dem iCloud- beziehungsweise iTunes-Backup ausschließen, falls Sie diesen Diensten nicht vertrauen. Schließlich legen Sie fest, wie lange die Sicherungsdateien behalten werden sollen - die Spanne reicht von einer Stunde bis zu "für immer". Außerdem lassen sich alle Backup-Dateien mit nur einem Tipp löschen.

Strongbox

Auch Strongbox installieren Sie über den App Store (siehe ct.de/y4ad). Die App begrüßt Sie mit einem gefälligen Willkommens-Pop-up und der Frage, ob Sie iCloud nutzen wollen, um Ihre Passwörter zu synchronisieren. Anschließend aktivieren Sie auf Wunsch das automatische Ausfüllen. Die angezeigten Anweisungen sind klar verständlich: Geräteeinstellungen öffnen, auf "Passwörter" tippen, dann auf "Automatisch ausfüllen", anschließend "automatisch ausfüllen" aktivieren und Strongbox auswählen.

Unabhängig davon, ob Sie diese Funktion aktivieren, müssen Sie erst mal Werbung für die Pro-Version über sich ergehen lassen. Ob Sie die kostenpflichtigen Funktionen wie Yubikey-Tokens und Mail-Support benötigen, können Sie 90 Tage gratis testen.

Datenbank erstellen

Sobald Sie eine neue Datenbank erstellen, fragt Strongbox nach einem Namen und gibt an, dass "Etwas Einfaches und Freundliches" ausreicht. Ob Sie nun aber "Passworthölle" oder "Gänseblümchen" eintippen, bleibt Ihnen überlassen. Nach einem Tipp auf "Weiter" geben Sie den Hauptschlüssel ein. Strongbox weist selbst darauf hin, dass das Passwort so gestaltet sein sollte, dass Sie es sich gut merken können und schlägt ein zufällig generiertes Passwort vor, das aus fünf englischen Wörtern besteht.

Ein Balken zeigt die Sicherheit des Passworts an. Nach dem Erstellen lässt sich das Passwort direkt ausdrucken und die Datenbank sofort öffnen. Sofern Sie die Cloud-Synchronisation nicht eingeschaltet haben, weist ein roter Text darauf hin, die Datenbank in der iCloud zu lagern und darüber zu synchronisieren.

< Schli	eßen		MvPasswords +		P	Beispieleintrag	Bearbeiten	
	Allger		Einstellungen	Fertig	Allgemein	Dateien Verlauf	15 million includes	
() ()	ntern	PREM	NUM				in Bindun	
	Email	*	Auf Premium aktualisieren	>			nativingiture	
(So F	inan:	-Q-	Neuheiten	>			•	
	Vetzv	App is Stund	it nützlich: 2 Stunden/Monat, das sind etwa len/Jahr.	28	issium.com		Z	
Ô	Betrie	STAR	T					
	Beisp	¢D	Automatisches Öffnen der vorherigen Datenbank	0	ich einige Noti	zen speichern, wenr	n Sie möchten.	In den Kee- passium-
Pr	Veuer	1.1.					0	Finstellunge
Cr.		8	Erscheinungsbild	>			the start start	findet
		•	Passwörter automatisch eintrager	n >			de finistro	der Nutzer
		Q	Suche	>				weitere

Im Datenbankmenü von Strongbox können Sie über das blaue Plussymbol weitere Datenbanken anlegen. Dabei haben Sie die Wahl zwischen "Express" und "Erweitert" – bei Letzterem können Sie den Speicherort selbst bestimmen, eine zusätzliche Schlüsseldatei oder einen Hardwareschlüssel anlegen und das Datenbankformat ändern. Strongbox unterstützt KDBX 4 und 3.1, KDB von Keepass 1.x und PSAFE3 3.x des Managers Password Safe 3.

Einträge bearbeiten

Strongbox packt lokale Datenbanken und Dokumente ins Apple-Backup, jedoch nicht die importierten Schlüsseldateien – das ist eine sinnvolle Voreinstellung, denn Schlüsseldateien sollten immer an einem anderen Ort gelagert werden als die Datenbank, ansonsten bieten sie keinen zusätzlichen Schutz.

Neue Datenbanken enthalten eine Beispielgruppe und einen Beispieleintrag. Einträge bestehen unter anderem aus Standardfeldern wie Benutzername, Passwort und URL. Ein Tipp darauf befördert sie in die Zwischenablage. Verglichen mit Keepassium bietet Strongbox einige Felder mehr. So lassen sich etwa Tags für Einträge vergeben oder Ablaufdaten festlegen – ab diesem Zeitpunkt wird der Eintrag nicht mehr berücksichtigt und ausgegraut dargestellt. Zudem lassen sich Notizen und benutzerdefinierte Felder hinzufügen, ein Einmalpasswort einrichten und Dateien anhängen – das kann aber auch Keepassium:

Strongbox schlägt auf Wunsch für alle möglichen Zugänge zufällige Benutzernamen und Passwörter vor. Ein langer Tipp auf das Aktualisierungssymbol über dem Passwortfeld öffnet ein Menü, in dem Sie aus verschiedenen Vorschlägen wählen können. In den Einstellungen entscheiden Sie sich für den Standard- oder den Diceware-Algorhitmus. In ersterem legen Sie die Länge des Passworts fest und aus welchen Zeichen es bestehen soll. Im Diceware-Modus reiht Strongbox mehrere Wörter aus einer Wortliste zufällig aneinander. Sie können die Trennzeichen wählen, die Länge bestimmen und Leetspeak aktivieren. Dann ersetzt der Generator Buchstaben durch ähnlich aussehende Zahlen und Zeichen-etwa 1337 statt leet. Sogar verschiedene Wortlisten und unterschiedliche Sprachen sind möglich.

Einstellungen

Über das Dreipunktmenü können Sie neue Einträge oder Gruppen anlegen. Hier durchsuchen Sie die Datenbank, ändern ihre Sortierung und Ansicht – etwa, ob Icons zu sehen sein sollen, welches Element grau als Untertitel unter den Einträgen erscheint und so weiter. Sie können außerdem die Datenbank exportieren, das Masterpasswort ändern oder Touch-ID dafür einrichten. Letzteres funktioniert allerdings nur in der Pro-Version.

Über den letzten Menüpunkt öffnen Sie die Datenbankeinstellungen. Hier ist vor allem der Punkt "Datenbank-Audit" interessant: Strongbox überprüft etwa, ob Passwörter in den Einträgen doppelt vorkommen und ob Sie leicht zu erratende Passwörter verwenden. In der Pro-Version gleicht die App die eingegebenen Daten mit der Leak-Datenbank "Have I been Pwned" ab. Findet Strongbox eine Übereinstimmung, warnt es den Nutzer. Somit lassen sich Datenabflüsse und Kaperungen von Online-Shop-Konten verhindern.

Über die Datenbank-Auswahl gelangen Sie zu den Haupteinstellungen: Blaues Zahnrad oben rechts neben dem Plussymbol antippen. Hier können Sie den Passwortgenerator aufrufen oder den Algorithmus und die Sicherheit für generierte Passwörter verändern. Außerdem können Sie einstellen, ob die Zwischenablage nach einer definierten Zeit automatisch gelöscht werden soll. Voreingestellt sind anderthalb Minuten. Weitere Optionen finden Sie in den erweiterten Einstellungen. Dort richten Sie etwa eine Web-DAV-Verbindung ein und lassen Tastaturen von Drittanbietern zu.

Fazit

Mit Strongbox und Keepassium können Sie Ihre Keepass-Passwörter auch auf Ihren iOS-Geräten anzeigen und verwalten – was



Die Dialoge von Strongbox richten sich eher an Einsteiger.

Keepass noch nützlicher macht. Da beide Apps nach wie vor weiterentwickelt werden, dürften sie wohl nicht so schnell aus dem App Store verschwinden.

Strongbox ist etwas einsteigerfreundlicher als Keepassium und führt Sie über ausführliche Dialoge und gute Erklärungen zum Ziel. Praktisch ist der eingebaute Diceware-Generator, mit dem Sie lange, gut merkbare Passwörter erzeugen. Die App nervt aber konstant mit Werbung für die Pro-Version. Das bleibt Ihnen bei Keepassium weitestgehend erspart. Außerdem entsperren Sie Keepassium selbst in der kostenlosen Version auf Wunsch mit biometrischen Merkmalen anstelle des Masterpassworts. Probieren Sie es einfach aus, welche App Ihnen am meisten zusagt. (abr@ct.de) dt

Weitere Infos: ct.de/y4ad

Dieser Artikel erschien ursprünglich auf heise+.

Tipp: Tippen und halten um Optionen anzuzeigen	Tipp: Zum Kopieren antippen, um Anmerkungen zu kopieren doppelt tippen				
Schließen Datenbank 💮	Abbrechen Beispiel	Fertig			
Q Suchen	Beispiel				
Beispielgruppe (0) Beispiel Benotzensante	Benu Benu Benu Bette wahlen Sie ihre bevorzugte Zeichenfolge jon Reserver-Umblen-Clad-Lindsum Mobile	0 0 0			
	mikki.horger Uni. https: 1273426718	Schwach (14 / 34.4 bits / 11a)			
	Tags trevals/38@yahoo.co.uk Tags capable				
	23.01 Neu generieren 18 Abbrechen	8			
	• TOTP einrichten				
	Neues benutzerdefiniertes Feld Anmerkungen				

Wer schnell irgendeine Zeichenfolge braucht, generiert in Strongbox eine mit zwei Tipps.