Passwortmanager auf Mobilgeräten

Quivive

Kai König, Diane Sieger

Nutzer von Mobilgeräten sind zwangsläufig online unterwegs und haben in der Regel eine Reihe von Passwörtern vergeben. Passwortmanager helfen dabei, den Überblick zu behalten.

In den frühen Jahren der elektronischen Kommunikation kamen viele Dienste ohne Passwörter aus – man konnte damals ja fast noch die Mehrzahl der anderen Internetnutzer im Wissenschaftsumfeld persönlich kennen. Massenkommunikation via E-Mail und Chat sowie die Notwendigkeit, vertrauliche Daten zu schützen, machten Logins und individuelle Passwörter obligatorisch. Heutzutage gilt bereits das Verwenden eines einzigen Passworts für mehrere Dienste als Sicherheitsrisiko.

Es gibt verschiedene Wege, mit diesem Problem umzugehen. Ein gängiger Ansatz basiert auf der Verwendung eines Passwortmanagers. Diese Tools sind im Umfeld von Desktop-Computern mehr oder weniger im Massenmarkt angekommen und als Desktop-Anwendungen verfügbar. In der Praxis nutzen viele Anwender Passwortmanager allerdings über die Integration mit Browsererweiterungen wie Chrome Extensions oder Firefox Add-ons.

Eins für alle

Auf Mobilgeräten sieht die Situation ein wenig anders aus. Hier liegen die meisten Passwortmanager als separate Apps vor und das Konzept von Browsererweiterungen wie auf dem Desktop existiert in vielen Fällen nicht für Mobilbrowser.

Einer der beiden Platzhirsche im Markt für Mobilgeräte ist „1Password“. Diese App verrät ihre Arbeitsweise bereits in ihrem Namen: Der Benutzer benötigt nur ein einziges Passwort, um Login-Daten, Lizenzen, Kreditkarten und Zugangsinformationen zu Bankkonten zu verwalten. Hinter diesem Master-Passwort sind persönliche Daten in Sicherheit.

Es lohnt sich also, ein möglichst langes und komplexes Master-Passwort zu wählen. Damit man dies nicht bei jeder Nutzung umständlich auf dem Mobiltelefon eintippen muss, erlaubt 1Password die alternative Authentifikation via Touch-ID. Das funktioniert auf modernen iOS-Geräten problemlos und zumindest auf dem Google Pixel 1 der Autoren auch unter Android. Einige Gerätehersteller sprechen Fingerabdrucksensoren auf Android über proprietäre APIs an, und man kann daher nur schwer generelle Aussagen über Kompatibilität treffen.

Doch 1Password kann mehr als nur Passwörter verwalten. Die App ermöglicht auch das Erzeugen neuer Passwörter. Die Regeln – etwa die Länge des Passworts, die Nutzung von Buchstaben, Ziffern, Symbolen oder Wortketten – legt der Anwender vorher fest. Wer die Anwendung zusätzlich auf dem Desktop-Computer oder Laptop nutzt, kann dafür auf eine der vielen Browser-Extensions (zum Beispiel für Chrome, Safari, Firefox oder Internet Explorer/Edge) zurückgreifen. Über sie kann 1Passwort dem Anwender ein Login in Onlineservices zur Verfügung stellen, das nur einen Klick erfordert.

Auf mobilen iOS-Geräten funktioniert das Login mit einem einzigen Klick ebenfalls. Öffnet man den Login-Bildschirm von Apps wie Slack, Dropbox, Kickstarter, Chefkoch, Spotify oder eBay – um nur einige zu nennen –, schlägt 1Password die korrekten Login-Daten vor. Auch Two-Factor-Authentication lässt sich in 1Password integrieren und man kann Codes aus der App heraus direkt abrufen. Die sogenannten Password-Vaults lassen sich auf verschiedene Arten synchronisieren, um auf unterschiedlichen Geräten zur Verfügung zu stehen, beispielsweise via Dropbox, iCloud oder lokalem WLAN. Natürlich kann man auch den Cloud-Service des Herstellers nutzen.

Ein besonders gelungenes Feature von 1Password ist der Security Audit. Er bietet dem Anwender mehrere Möglichkeiten, sicherzustellen, dass ein Passwort wirklich sicher ist. Watchtower beispielsweise identifiziert Dienste, von denen bekannt ist, dass sie kürzlich gehackt wurden. Auch schwache Passwörter kann die App anzeigen. Auf Wunsch erzeugt sie Übersichten mit mehrfach verwendeten Passwörtern. Zusätzlich gibt es eine Übersicht von Login-Daten, die der Nutzer seit mehr als sechs Monaten, einem Jahr oder gar drei Jahren nicht mehr geändert hat. Somit fällt das regelmäßige Aufräumen der Passwörter wesentlich leichter.

Träger der Apple Watch können definieren, welche Passwörter sie über die Uhr abrufen möchten. Dies bietet sich besonders bei kürzeren Sequenzen an, die oft auf die Schnelle hervorgeholt werden müssen, etwa Kreditkarten-PINs oder Codes für Two-Factor-Authentication.

1Password kann man 30 Tage kostenlos ausprobieren, danach wird ein Abonnement fällig. Preislich kann eine Einzelperson mit 2,99 US-Dollar pro Monat starten, für Familien, Teams und Businesskunden gibt es Pläne, die auf deren unterschiedliche Bedürfnisse zugeschnitten sind. Für diesen Artikel wurde die Version 6.8.9 der App getestet. Version 7 gibt es bereits als Beta.

An den Notfall denken

Der zweite verbreitete Passwortmanager ist „LastPass“. Die App spielt in derselben Liga wie 1Password. Viele Features sind ähnlich, beispielsweise die Synchronisation zwischen Mobil- und Desktop-Geräten, zur Verfügung stehende Zwei-Faktor-Authentifizierung und das Login per Fingerabdruck. Die Unterschiede liegen eher im Detail.

So kann man mit LastPass etwa für den Notfall Familienmitgliedern oder Freunden den Zugriff auf die persönliche Passwortdatenbank erlauben. Eine vertraute Person, die ebenfalls LastPass-Nutzer sein muss, kann bei Bedarf Passwörter und Login-Daten ansehen und einsetzen. Hierfür muss die definierte Person den Zugriff anfordern – erfolgt kein Wider-

spruch innerhalb eines zuvor festgelegten Zeitrahmens, kann der Notfallkontakt alle Daten in die eigene App einlesen.

Installiert man LastPass auch auf dem Desktop-Computer, kann man Browser-Add-ons für Chrome, Safari und Firefox gleich mit installieren. Kleine Warnung für all diejenigen, die gern unzählige Browsertabs gleichzeitig geöffnet haben: Während der Installation werden alle gewählten Browser geschlossen und neu gestartet.

Für Android-Nutzer ist vielleicht interessant, dass LastPass ein Add-on für Firefox Mobile bietet. Wie in der letzten Ausgabe der App-Infos nachzulesen, handelt es sich dabei um einen der wenigen Mobilbrowser, der Erweiterungen unterstützt.

LastPass kostet 24 US-Dollar pro Jahr in der Premiumversion, als Familie kann man sich bis zu sechs Lizenzen für 48 US-Dollar sichern. Weitere Abonnements stehen für Teams und auf Enterprise-Level zur Verfügung, jedoch kann ein durchschnittlicher Nutzer auch gut mit den nur wenig eingeschränkten Features der kostenfreien Version zurechtkommen.

Wer mehr Flexibilität will und an einer Open-Source-Lösung interessiert ist, sollte sich die „KeePass"-Plattform anschauen. Die App stellt im Kern nur eine Windows-Lösung dar. Auf Linux oder macOS läuft sie mithilfe von Mono oder Wine, was zusätzliche Schritte bei der Einrichtung erfordert. KeePass richtet sich daher eher an ambitionierte und technisch versierte Nutzer.

Mit über 100 Plug-ins lässt sich die Desktop-Version an nahezu alle Anwenderbedürfnisse anpassen. Darunter findet man Module zur Integration mit Browsern, aber auch Im- und Exporterweiterungen oder Anbindung an Cloud-Dienste zum Synchronisieren von Passwortdaten sind im Angebot. Insbesondere die Offenheit des Quellcodes stellt für viele ein schlagendes Argument dar, da sie damit nicht auf Code in einer proprietären Blackbox angewiesen sind.

„MacPass" ist eine macOS-native Alternative zu KeePass, die keine Laufzeitumgebungen wie Mono oder Wine erfordert. Die App ist KeePass-kompatibel. Dieser Begriff bezieht sich in der KeePass-Community in der Regel auf Kompatibilität auf der Ebene der Passwortverwaltung – MacPass kann die KeePass-Plug-ins nicht nutzen. Trotz allem ist MacPass eine gut gelungene macOS-App, die auf Bibliotheken aus KeePass basiert und ebenfalls als Open Source verfügbar ist.

Für Mobilgeräte gibt es keine offiziellen KeePass-Apps, sondern Community-Entwicklungen. Durch das gelungene Material-Design-UI und die einfache Nutzung fällt hier „Keepass2Android" positiv auf. Wie MacPass ist diese App KeePass-kompatibel.

Sicher im Safe

Auf Wunsch kommt Keepass2Android mit eigenem Screen-Keyboard, was einem möglichen Angriffsvektor durch Tastatur-Apps vorbeugt.

Möchte man das KeePass-Ökosystem auf iOS nutzen, bietet sich „MiniKeePass" an. Die kostenlose App kommt in einem übersichtlich und klar designten, minimalistischem Layout und ist im Wesentlichen Feature-kompatibel mit Keepass2Android. (ka@ix.de)

Alle Links: ix.de/ix1807136

Vor 10 Jahren: Schluss mit lustig

Vor zehn Jahren war „Schluss mit lustig". Das verkündete das Editorial der *iX* 7/2008. Erstmals war ein deutscher Hacker für das unerlaubte Eindringen in fremde Netze mithilfe des bedrohlich klingenden „Wardrivings" verurteilt worden.

Der deutsche WLAN-Hacker fuhr nicht herum und stöberte nach ungesicherten Netzen, sondern nahm den Weg über das ungesicherte WLAN seines Hausnachbarn. Egal. Das Amtsgericht Wuppertal verurteilte den Mann für die „unerlaubte WLAN-Nutzung", doch die Strafe war eher symbolisch. Der Laptop wurde eingezogen, verbunden mit der Warnung, dass im Wiederholungsfall 20 Tagessätze fällig seien. Das Gericht begründete das milde Urteil damit, dass die Rechtslage „bislang ungeklärt" gewesen sei. Deswegen gab es nur eine „Verwarnung mit Strafvorbehalt", juristisch gesprochen.

Interessant war die Einschätzung des Gerichts, dass die vom WLAN-Router des Nachbarn zugewiesene IP-Adresse eine abgehörte Nachricht darstelle, weshalb der Wardriver auch gegen das Bundesdatenschutzgesetz verstoßen habe. Im *iX*-Editorial sah Jürgen Seeger darin einen interessanten Ansatz, sich den Herausgabeansinnen von Sicherheitsbehörden zu widersetzen.

Der *iX*-Chefredakteur sah aber noch ein ganz anderes Problem: „Und wie soll in der Logik des Wuppertaler Urteils ein Fall gewertet werden, bei dem sich ohne Zutun des Benutzers sein Rechner mit dem nächsterreichbaren WLAN verbindet? Will man auch dem unerfahrenen User eine aktive Prüfungspflicht aufbürden?"

Zehn Jahre später ist das Problem gelöst, freilich in einem ganz andere Sinne. Mit dem Wegfall der „Störerhaftung" darf man sich mit offenen WLANs verbinden, ohne sich damit schuldig zu machen. So ist das Wardriving als „Hackersport" ziemlich in Vergessenheit geraten.

Gleichzeitig ist die Nutzung der Technik jedoch krimineller geworden: Zum gezielten Ausspionieren werden in Hotels oder Firmen WLAN-Router mit identischen WLAN-Namen eingerichtet, mit denen sich dann Geräte arglos verbinden, weil sie den WLAN-Namen gespeichert haben. Im aktuellen Verfassungsschutzbericht – dieser Dienst ist für Wirtschaftsspionage zuständig – stehen solche Angriffe im Ausland an zweiter Stelle der Angriffstaktiken fremder Unternehmen und Staaten. (Nummer eins ist das Filmen von Sex über die Kamera im TV.)

Oder stehen wir heute vor einem ganz anderen Problem? In diesen Tagen warnte der Bund für Umwelt und Naturschutz Deutschland vor den Strahlengefahren im Kinderzimmer. Jungen Eltern wird von der Industrie eine Vielzahl von Geräten jenseits des Babyphones angedient, die sich automatisch mit dem WLAN verbinden wollen. Es gibt smarte Schnuller und Windeln mit Nässemelder, die ins WLAN wollen, weil Bluetooth Low Energy nur einen Raum weit reicht.

Blättert man in der BUND-Broschüre, liest man von vielen Anwendungen, die die Welt nicht braucht und bei denen die Umweltschutzorganisation eine Strahlenbelastung für in Entwicklung befindliche Hirne befürchtet. Das fängt beim drahtlosen Wehen-Messegerät für Schwangere an, das sich mit jedem WLAN zu verbinden versucht. Die Organisation spricht von einer Strahlengefahr, vor der nicht ausreichend auf den Produkten gewarnt wird. *Detlef Borchers* (js@ix.de)