Wie man Passwort-Manager richtig benutzt

von „Jay“ auf securityspread.com, Übersetzung: KJM

Ich habe **1Password** schon früher erwähnt. Es ist in meinen Augen der beste Passwort-Manager, den es für Mac und iOS gibt. Wenn Sie nicht mit ihm vertraut sind, empfehle ich sehr, es auszuprobieren und – je früher, desto besser – zu beginnen, es zu benutzen.

Wenn Sie 1Password bereits nutzen oder erwägen, das künftig zu tun, dann ist dieser Artikel etwas für Sie.

Ein Passwort-Dienstprogramm wie 1Password zu nutzen, ist ein großer erster Schritt. *„Gibt's denn noch mehr Schritte?“* – Absolut. Das Ersetzen von Klebezetteln oder eines Kontakts im Adressbuch mit Namen „Passworte“ *(ich habe so etwas schon gesehen …)* durch einen Passwort-Manager ist ein guter Anfang, aber es gibt einen richtigen und einen falschen Weg, ihn zu benutzen. In diesem Artikel werde ich einige Methoden beschreiben, Passworte instand zu halten und Ihre Passwort-Strategie generell zu verbessern.

Benutzen Sie den Passwort-Manager wirklich!

Ich habe viele Anwender gesehen, die 1Password installierten und alle Passworte eingaben, an die sie sich in dem Moment erinnerten, und die das Programm später nie wieder angefasst haben. Nach einer Weile vergaßen sie ihr Master-Passwort oder aber sie benötigten später ein Passwort, das sie niemals in 1Password eingegeben hatten. Wenn Sie sich entschließen, einen Passwort-Manager zu nutzen, dann benutzen Sie ihn auch. Akzeptieren Sie die Tatsache, dass es eine kleine Lernkurve gibt und dass es die Art und Weise ändern wird, wie Sie mit Ihrem Computer umgehen. Nach wenigen Tagen werden Sie sich aber fragen, wie Sie zuvor ohne Passwort-Manager ausgekommen sind.

Nutzen Sie all seine Funktionen!

Ein guter Passwort-Manager ist viel mehr als nur das. 1Password kann Passworte speichern, Kreditkarten, Software-Lizenzen und noch mehr. Wenn es das schon tun kann, dann nutzen Sie es auch. Es wird Ihr Leben einfacher und sicherer machen. Warum sollte man Passworte sicher speichern, aber Kreditkarten auf dem Tisch herumliegen lassen? Ich speichere alles Wichtige in 1Password, sodass ich immer weiß, wo ich es wiederfinde, und ich weiß, dass ich der einzige bin, der darauf zugreifen kann. Indem ich die eingebaute Synchronisation auf all meinen Geräten nutze, stehen meine Passworte, sicheren Notizen, Router-Logins und Kreditkarten-Informationen auf auf all meinen Computern oder meinem iPad oder iPhone zur Verfügung.

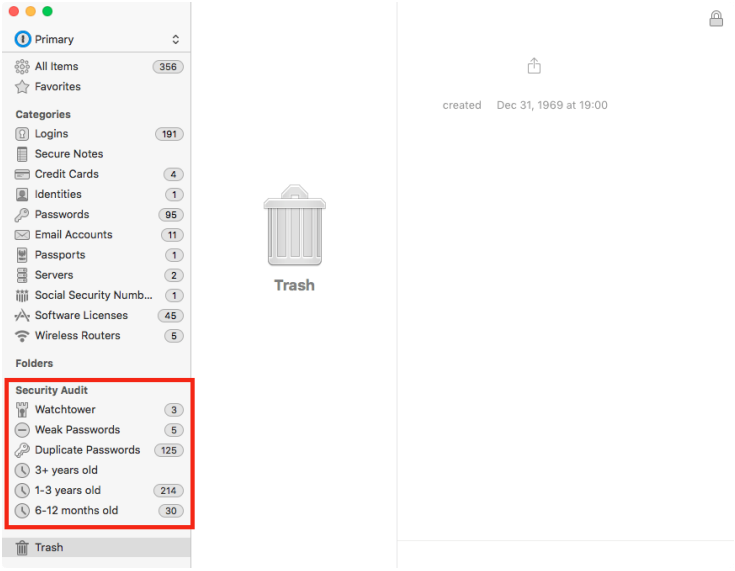
Wissen, wo man's findet …

Übertragen Sie jedes gespeicherte Passwort in Ihren Passwort-Manager. Ihr Browser speichert Passworte für Sie. Welches Passwort ist wo gespeichert? Werden diese Passworte auf sichere Weise auf Ihre anderen Geräte synchronisiert? Eine alarmierende Menge Leute benutzt immer noch Notizzettel oder andere unsichere Methoden, Passworte zu speichern. Wo haben Sie das Passwort für diesen oder jenen Service aufgeschrieben? Passworte an *einem* Platz zu speichern, stellt sicher, dass Sie jedes Passwort dann zur Verfügung haben, wenn Sie es brauchen. In Ihren Browsern (durch die 1Password-Erweiterung) sowie auf Ihren anderen Geräten (durch Synchronisation), und das ist so sicher, wie es überhaupt sein kann.

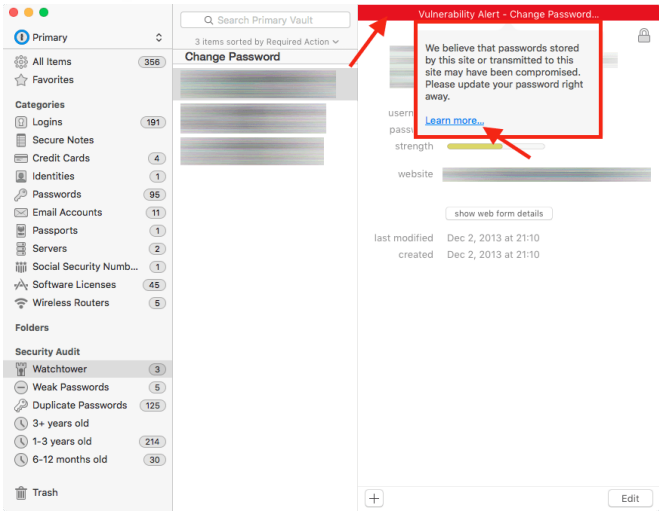
Nun wollen wir einen Blick in den Passwort-Manager werfen, um zu sehen, wie er auf die beste Weise genutzt wird und ob die Sicherheit durch ein paar Wartungsmaßnahmen noch verbessert werden kann.

Prüfung auf bekannte Schwachstellen

Starten Sie 1Password und schauen sie nach unten in der linken Spalte. Suchen Sie das Wort „Sicherheitsüberprüfung“; die erscheint zunächst noch geschlossen. Klicken Sie auf den kleinen „Anzeigen“-Button rechts daneben, um alle Optionen anzeigen zu lassen.



Dort ist nämlich der richtig gute Stoff verborgen. Die oberste Option heißt *Watchtower*. Watchtower prüft die URL, die Sie in Ihrer Passwort-Notiz gespeichert haben, und meldet Ihnen, ob es dort in der Vergangenheit Schwachstellen gab oder gar aktuell gibt.



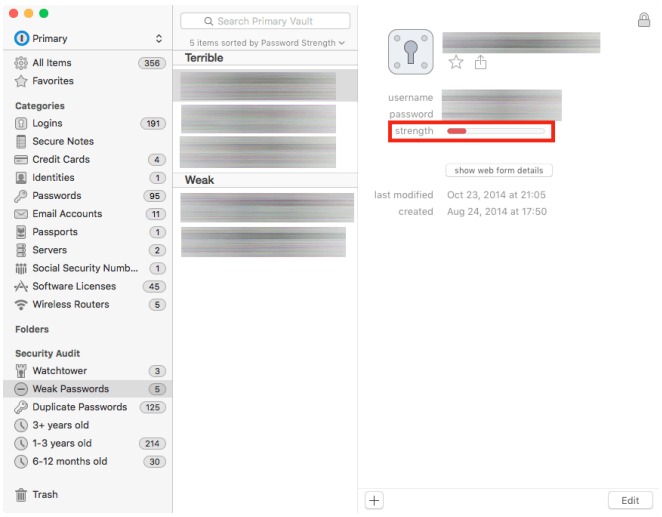
WARNHINWEIS: ÄNDERN SIE IHRE PASSWORTE NIE NUR IM PASSWORT-MANAGER! Denn so überschreiben Sie Ihr altes Passwort, und woher soll die betroffene Webseite wissen, dass Sie ab sofort ein anderes Passwort verwenden wollen? Es besteht die Gefahr, dass Sie Ihr Log-in komplett einbüßen.

Loggen Sie sich also erst einmal mit dem alten Passwort auf der Website ein und ändern Sie dort Ihre Zugangsdaten (gern mit Hilfe des Passwort-Generators). Die 1Passwort-Browser-Erweiterung ist eine große Hilfe. 1Passwort erkennt, dass für diese Website bereits ein Eintrag gespeichert war, und fragt nach, ob das alte Passwort durch das neue ersetzt werden soll. – KJM –

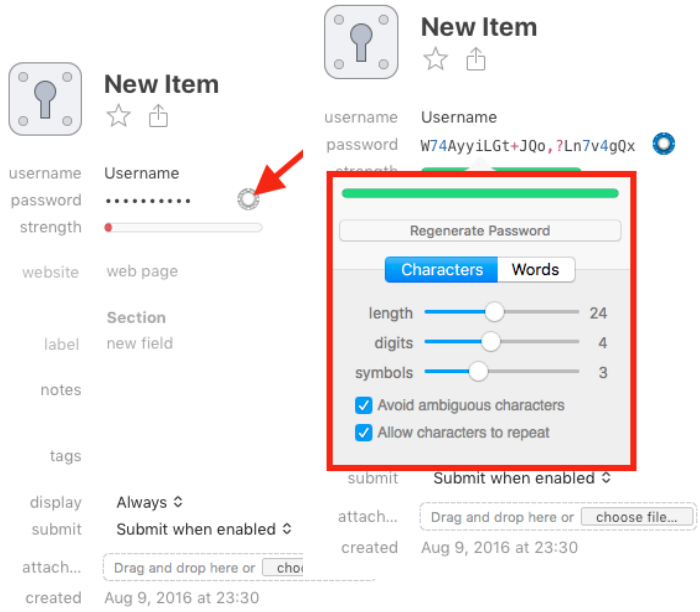
Wenn dort im *Watchtower* Einträge aufgelistet sind, wählen Sie sie aus und klicken Sie das rote Banner in der rechten Spalte an. Eine kleine Erklärung öffnet sich mit einem „Erfahren Sie mehr"-Link. Es ist typischerweise eine gute Idee, der Empfehlung zu folgen und das Passwort für diese Website zu ändern. (Ich habe dort allerdings ein paar Sites aufgelistet gesehen, bei denen ich nicht erkennen konnte, warum 1Password meint, dort sei vielleicht ein Problem. Urteilen Sie nach eigenem Ermessen, wenn Sie auf eine solche Website stoßen.

Schwache Passworte

Mit der Möglichkeit, wahnsinnig lange und komplexe Passwörter in 1Passwort zu generieren, sollte diese Kategorie immer leer sein. 1Password erinnert sich für Sie an diese Passwörter; daher gibt es keinen Grund, nur Passwörter zu verwenden, an die Sie sich selbst erinnern können! Schauen Sie sich die aufgelisteten Einträge an, wenn es welche gibt, und die Anzeige der Passwort-Stärke zeigt Ihnen unmittelbar an, ob ein neues Passwort sinnvoll ist.



Bei diesen Einträgen klicken Sie den „Bearbeiten"-Button und tragen ein neues Passwort ein. Ich empfehle, den eingebauten Passwort-Generator zu nutzen und das neue Passwort so zu wählen, dass Sie selbst im Leben nicht darauf kommen würden. Sie können das tun, indem Sie das Icon direkt neben dem Passwort-Feld anklicken.



Heutzutage bestehen meine Passworte aus mindestens 20 Zeichen und beinhalten viele Symbole und Ziffern. Lässt man Zeichen-Wiederholungen zu, ist das technisch zwar unsicherer, aber in Passworten dieser Komplexität spielt ein wiederholtes Zeichen wohl kaum eine Rolle. — Benutzen Sie denselben Passwort-Generator, wenn Sie Passwort-Duplikate bereinigen; grundsätzlich sollte es gar keine Duplikate geben.

Die letzten drei Kategorien sortieren die gespeicherten Passwörter nach ihrem Alter. Abhängig davon, wie oft – wenn überhaupt – Sie Ihre Passwörter ändern, ist das sehr hilfreich. Ich versuche, meine Passwörter einmal im Jahr zu ändern, sodass ich besonders auf die Kategorie „1-3 Jahre alt" achte.

Nachdem wir die Sicherheitsüberprüfung durchgeführt haben, was kann man noch tun?

Alte Passwörter löschen

Gehen Sie Ihre Passwort-Liste durch und suchen Sie Dienste, für die Sie sich vor Jahren registriert haben, die Sie aber seit langem nicht mehr benutzt haben. Besuchen Sie deren Website und schauen Sie, ob Sie Ihren Account dort komplett löschen können. Hier kann ein Service wie justdelete.me helfen.

Prüfen Sie alle übrigen gespeicherten Einträge

Dienste und Websites, bei denen Sie sich früher einmal angemeldet haben, können mittlerweile andere oder zusätzliche Sicherheitsmaßnahmen nutzen. Prüfen Sie jeden Eintrag in Ihrer Liste und schauen Sie, ob dort jetzt z.B. *2 Factor Authentication* genutzt wird, etwas, was für jeden Dienst und jede Website genutzt werden sollte, wo es angeboten wird. Ebenso: Sind die mit Ihrem Passwort gespeicherten URLs http oder https? Die meisten Websites, die https anbieten, werden den Link automatisch weiterleiten, aber es ist besser, direkt auf der gesicherten https-Site zu landen.

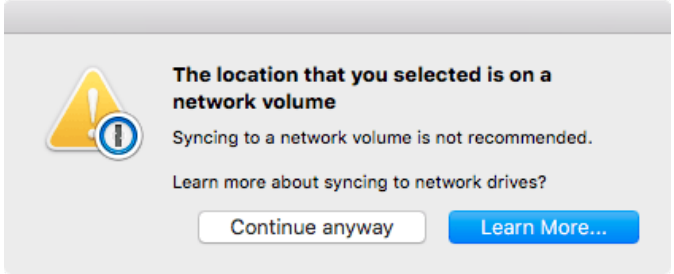
Eine Menge Websites benutzen Ihre Email-Adresse als Ihre Benutzerkonto-ID, wenn Sie sich registrieren. Prüfen Sie alle Einträge, dass tatsächlich eine aktuelle Email-Adresse verwendet wird. Wenn Sie sich bei einer Website vor Jahren mit einer Email-Adresse angemeldet haben, die heute nicht mehr existiert oder nicht mehr zugänglich ist, werden Sie es schwer haben, wenn Sie jemals Ihr Passwort zurücksetzen müssen. Firmen schreiben gelegentlich ihre Kunden an, wenn es Sicherheitsprobleme gegeben hat; ohne aktuelle Email-Adresse verpassen Sie diese wichtigen Updates.

Prüfen Sie das eine Passwort, an das Sie sich erinnern müssen!

Ihren Passwort-Speicher mit einem Passwort wie „Password 123" zu sichern, ist natürlich ebenso unsinnig wie fahrlässig. Vergewissern Sie sich, dass Sie ein ausreichend langes Master-Passwort verwenden, komplex genug, aber trotzdem leicht zu merken.

Backup Ihrer 1Password Datenbank

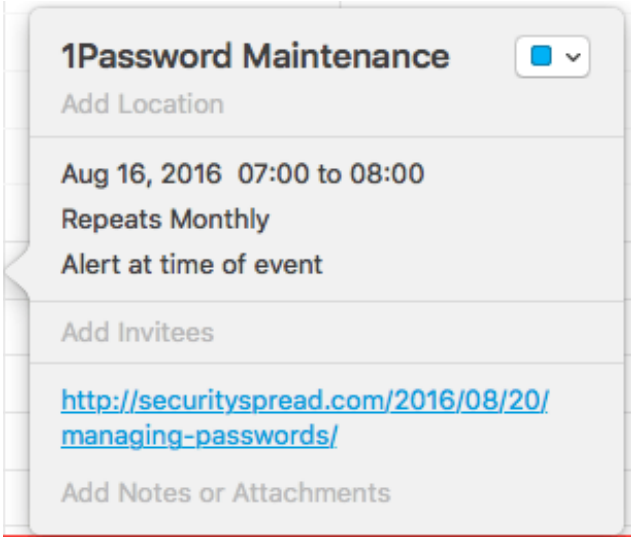
1Password speichert per Voreinstellung lokale Backups Ihrer Datenbank. Diese Backups können Sie im Ordner ~/Library/Application Support/1Password/Backups finden. Es ist eine gute Idee, daneben auch ein externes Backup zu haben. Öffnen Sie die Programm-Einstellungen und gehen Sie zum Synchronisieren-Tab. Hier haben Sie eine Option, Ihre Datenbank mit iCloud oder Dropbox zu synchronisieren. Sie können auch auf „Ordner" klicken und einen lokalen File Server wählen, obwohl das von 1Password nicht empfohlen wird.



Dieser Dialog ist ein netter Weg, zu sagen: „1Password wird total verrückt, wenn es diesen Fileserver nicht finden kann".

Erinnern Sie sich selbst daran, all das zu tun.

Legen Sie eine Erinnerung oder einen Kalender-Alarm an, der Sie daran erinnert, all diese Wartungsmaßnahmen regelmäßig jeden Monat oder alle paar Monate durchzuführen. Sie können sogar einen Link zu diesem Artikel hinzufügen, damit Sie sich nicht an alles beschriebene erinnern müssen. Nach einer Weile wird es Teil Ihrer Routine werden, und Sie werden diese Wartungsmaßnahmen von selbst durchführen, ohne einer Erinnerung zu bedürfen.



Anmerkung: Am Anfang mag das Eingeben der Informationen in die Datenbank ja mühsam sein, wenn man all seine „gesammelten Werke" erst einmal erfassen muss. Im täglichen Gebrauch wandelt sich das dann, denn neu generierte Passwörter werden mit der zugehörigen URL automatisch gespeichert, und man findet die Passworte über die 1Passwort-Browser-Erweiterung sehr komfortabel wieder.

1Passwort installiert außerdem eine Erweiterung in der Menüleiste, und so ist es nicht nur im Browser, sondern auch im Finder und in allen anderen Programmen möglich, rasch auf gespeicherte Informationen zuzugreifen – natürlich nur, wenn man das Master-Passwort kennt. *–KJM–*

Warum nicht einfach den Schlüsselbund verwenden anstelle von 1Password oder LastPass?

von Glenn Fleischmann, MacWorld. Übersetzung: KJM

Der OS X Schlüsselbund hat eine Menge exzellenter Eigenschaften, aber er ist nicht so einfach aufzurufen und auch nicht so vielseitig wie 1Password, LastPass, und andere Passwort-Ökosysteme von Drittherstellern.

Ich empfehle immer wieder, eine Art von Passwort-Management-System zu verwenden, die es erlaubt, schwer zu brechende Passworte anzulegen (ob sie nun kurz und kompliziert oder lang und einfach zu merken sind), jedenfalls einzeln für jede Website und jeden Dienst, und die es auch ermöglicht, diese Passworte überall dort einzugeben, wo sie benötigt werden.

Lowell Nelson fragte mich vor ein paar Wochen, warum ich so versessen sei auf Lösungen von Drittherstellern wie z. B. **1Password**, **Dashlane** und **LastPass**, obwohl Apple doch eine eigene robuste Multiplattform-Lösung habe, die auch Synchronisation beinhalte: den **Schlüsselbund**. („Schlüsselbund" bezeichnet genau genommen den OS-X-Teil, während „iCloud Schlüsselbund" die Synchronisation zwischen mehreren Geräten und die Nutzung in iOS ermöglicht.)

Das war eine wirklich gute Frage, und ich ziehe es vor, keine Kaufempfehlung für kostenpflichtige Dienste auszusprechen (egal, ob per Einmalzahlung oder Abonnement), wenn der Nutzwert dieses Dienstes nicht so groß ist, dass er die Kosten überwiegt.

Schauen wir uns die Details an. Da ich 1Password und LastPass intensiv ausprobiert und geprüft habe, benutze ich diese beiden als Vergleichsbasis. Sie, der Leser, sollten in der Lage sein, zu all den nachstehend aufgezählten Punkten Antworten in den FAQs oder Leistungsbeschreibungen aller entsprechend robusten Alternativen zu finden.

Während Apples Schlüsselbund, 1Password und LastPass diverse Arten von Informationen sicher speichern können, sind Passworte das am meisten vertrauensbedürftige Element, das in einem ganzen Ökosystem und auch über Plattformen hinweg genutzt werden kann.

Wie sicher sind Ihre Daten?

Ein Passwort-„Safe" muss die Passwörter, naja, *sicher* aufbewahren in drei größeren Bereichen:

- Daten, die auf (Mobil-)Geräten lagern. Passwörter sollten auf einem Gerät gegenüber jedem außer dem Eigentümer geschützt sein.
- Daten, die auf Servern liegen. Es sollte für Angreifer schwierig oder unmöglich sein, auf in der Cloud gespeicherte Passwörter zuzugreifen und sie zu entschlüsseln.
- Daten, die während der Synchronisation oder bei web-basiertem Zugriff transportiert werden. Eine starke Verschlüsselung sollte Schnüffler daran hindern, neue Einträge, Suchanfragen und Updates zu entziffern, ebenso wie die interaktiven Sessions.

Schlüsselbund und iCloud Schlüsselbund sind in dieser Beziehung verdammt robust. OS X und iOS müssen „entsperrt" werden, um Schlüsselbund-Einträge irgendwo einzugeben, und das Schlüsselbund-Verwaltungsprogramm von OS X fordert ein Administrator- oder Benutzer-Passwort an, um Passwörter in lesbarer Form anzuzeigen. Mit Touch ID oder einem Passcode in iOS und FileVault 2 in OS X sind die Passwörter stark geschützt sowohl in ausgeschaltetem Zustand (OS X) oder verschlossen (iOS). Der iCloud Schlüsselbund benutzt eine Geräte-basierte Verschlüsselung, was es Apple, selbst wenn es dazu verurteilt wird, unmöglich macht, Passwörter zu entschlüsseln.

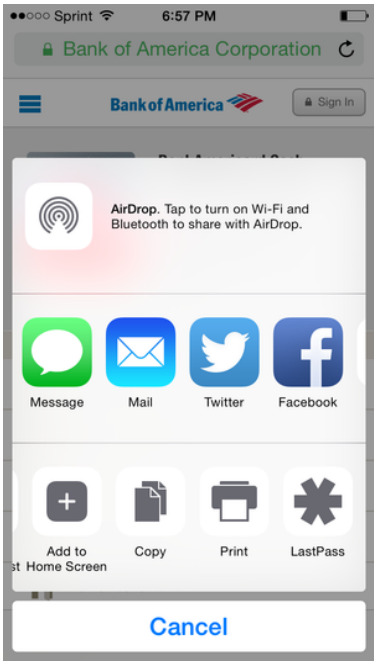
1Password und LastPass benutzen eine „aufwändige" Passphrasen-Verschlüsselungsmethode für ihre lokal gespeicherten Datenbänke, so dass selbst, wenn ein Hacker sie in die Finger bekommt, er nur Brute-Force-Attacken in sehr, sehr langsamer Geschwindigkeit versuchen könnte. LastPass hat das vor kurzem unabsichtlich – nach einem Hackerangriff – testen können: Es trafen tatsächlich keine Berichte über geöffnete Passwort-Safes ein.

LastPass synchronisiert alles über seine Server, aber verschlüsselt die Daten mit Schlüsseln, die nur dem Anwender bekannt sind. 1Password synchronisiert via Dropbox und über andere Cloud-basierte Dienste (vertrauend auf ihre Sicherheits- und Lagerungs-Verschlüsselungsmethoden) sowie durch sein ergänzendes Abonnementssystem der Freigabe für Familie oder Team-Mitglieder, aber sichert alles mit benutzereigenen Schlüsseln.

LastPass und die Team- oder Familien-Optionen für 1Password gewähren auch Zugriff über Web-Browser und benutzen Browser-basierte Verschlüsselung anstelle nativer Benutzer-Software; die Firmen besitzen nicht die Schlüssel der Benutzer. Dennoch ist es eine Schwachstelle, wenn man sich auf den Browser verlässt. Malware und andere Browser-basierte Exploits machen Browser viel verletzlicher, verglichen mit dem Sicherheitslevel, das durch native Apps und Cloud-Synchronisation zur Verfügung steht. Immer wieder entdeckt man Safari-Schwachstellen in iOS und OS X (obwohl nur sehr wenige tatsächlich in freier Wildbahn ausgenutzt werden), und man könnte in Versuchung geraten, von einer ungewohnten Maschine aus mit einem fremden OS auf Passworte zuzugreifen.

Wie einfach ist das System zu nutzen?

Ein Passwort-System muss einfach zu nutzen sein. Wenn es das nicht ist, wird man es nicht benutzen; so ist die menschliche Natur. Schlimmer noch: Wenn Sie es für jemand anderen installieren, um seine Sicherheit zu verbessern, wird derjenige es wahrscheinlich überhaupt nicht benutzen, wenn es nicht ein zuverlässiger Erinnerer ist und supereinfach zu bedienen.



iOS Apps unterstützen möglicherweise eher LastPass' und 1Password's Extensions als den iCloud Schlüsselbund.

Apple nutzt den Schlüsselbund in erster Linie als ein Weg, Passwörter für spezifische Felder auf Webseiten zu speichern, und Passwörter aufzubewahren für eine automatische Suche und als Abkürzung in seiner Software (wie AirPort Admin in OS X) oder für Dritthersteller-Software, die Apple's Schlüsselbund-Haken benutzt. In Safari, ob mobil oder Desktop, funktioniert der Schlüsselbund sehr gut, vom Vorschlagen starker Passwörter über das Speichern bis zur Möglichkeit, sie wieder hervorzuholen oder andere gespeicherte Alternativen zu benutzen.

Aber während der Schlüsselbund in OS X von weitreichendem Nutzen ist, zumal zahlreiche Entwickler ihn adoptiert haben und es die Schlüsselbund-Verwaltung für den direkten Zugriff und die Passwortsuche gibt, muss man in iOS umständlich tief in `Einstellungen > Safari > Passwörter` graben, um Passwörter anzuschauen, sie zu bearbeiten oder auch (ganz nach unten wischen!) um Passwörter hinzuzufügen. Außerdem kann man den Schlüsselbund nicht in Dialogen außerhalb des Webs aufrufen, was ihn für allgemeine Zwecke nutzlos macht. Zwar können Sie im Bedarfsfall ein Passwort recht einfach erstellen, aber es ist schwer zu erreichen und kann nur auf der dazugehörigen Webseite bequem wiedergefunden werden.

Apple hat aber mit iOS 8 begonnen, Erweiterungen zuzulassen; diese erlauben es 1Password, LastPass und anderen Werkzeugen, in Safari und auch in anderen Apps aufgerufen zu werden. Viele iOS Apps, die ich benutze, sind direkt mit 1Password's API verbunden, was ein direktes Aufrufen erlaubt. Im schlimmsten Fall kann ich immer noch zu LastPass oder 1Password wechseln, um das Passwort zu finden, es zu kopieren, dann zur App zurückkehren und das Passwort dort einfügen.

Man kann die App auch dazu benutzen, starke Passwörter zu erzeugen, die beim Erzeugen sofort gespeichert werden, automatisch synchronisiert werden und in die Zwischenablage kopiert werden können, um sie in andere Apps einzusetzen.

1Password kann Ihre Passwörter sogar auf Ihre Apple Watch bringen, wenn Sie ein Pro User sind, und auch LastPass hat eine Apple Watch App.

Die Cross-Plattform-Situation ist viel schlechter. Apple stellt den iCloud Schlüsselbund außerhalb der eigenen Betriebssysteme nicht zur Verfügung. 1Password und LastPass hingegen (andere Apps auch) sind auf einer breiten Vielfalt größerer Plattformen verfügbar; zusätzlich bieten sie Browser-basierten Zugriff (voreingestellt bei LastPass und als Abo-Option bei 1Password).

Der iCloud Schlüsselbund bietet keinen Mechanismus, Informationen mit anderen Leuten zu teilen — Teil der andauernden Geschichte, die ich seit Jahren diskutiere darüber, dass Apple seine Systeme nicht von Grund auf daraus auslegt, zu erkennen, dass Leute in Gruppen und als Familien arbeiten. (Lassen Sie mich gar nicht erst anfangen von den Problemen mit der Familien-Freigabe.)

Die meisten Passwort-Systeme haben einen Mechanismus, Geheimnisse mit Anderen zu teilen, die über Benutzerkonten angemeldet sind. 1Password erlaubt die direkte Übermittlung ohne ein Abonnement oder, seit kurzem, die ausgewählte Freigabe unter Mitgliedern von Geschäfts- oder Familiengruppen. LastPass bietet das, da die Einträge zentral gelagert werden, schon seit Jahren an.

Was wählt man denn nun?

Wenn Sie Passwörter fast ausschließlich auf Webseiten benötigen, nur iOS und OS X benutzen und wenn es Ihnen nichts ausmacht, die Passwörter einzutippen, die Apple für seine Dienste anfordert, erfüllen Schlüsselbund und iCloud Schlüsselbund die Anforderungen. Wenn nicht alle diese Bedingungen auf Sie zutreffen, lohnt sich das Investment in ein Passwort-Management-System.

Verborgene Schätze im macOS:

15 Tastenkombinationen für den Start des Macs

von Josh Centers, tidbits.com, Übersetzung KJM

Wenn die sprichwörtliche Scheiße auf den Ventilator trifft und Ihren Mac daran hindert, so zu starten, wie Sie das wollen, kann es Ihren Hintern retten, wenn Sie die richtige Tastenkombination für den Start des Macs kennen, nämlich, ob Sie in den Safe Mode starten wollen oder in die Recovery Partition, Apple Diagnostics oder von einer ganz anderen Disk.

Hier sind fünfzehn Startup Key Kombinationen, die den Tag retten können, wenn Dinge schief gehen. Nicht alle sind auf aktuellen Macs noch von Nutzen, aber wir wollen die Liste komplett darstellen.

Option: Startup Manager — Die erste Start-Taste, die jeder Mac-Anwender kennen sollte, ist die Optionstaste ⌥ . Wenn Sie die Optionstaste beim Start des Macs drücken und halten, öffnet sich der Startup Manager, der es ermöglicht, auszuwählen, von welcher Disk man starten möchte.

Der Startup Manager ist in erster Linie nützlich, um von einem anderen Laufwerk aus zu starten wie einem Klon des Systems, einem USB-Stick oder einer Boot Camp Partition. Man kann ihn aber auch benutzen, um den Start von Ihrem Hauptlaufwerk zu erzwingen, wenn Ihr Mac hartnäckig von einer anderen Disk aus startet. Der Startup Manager kann auch helfen, eine unzuverlässige Festplatte zu identifizieren; wenn das Laufwerk, das Sie suchen, nicht im Startup Manager erscheint, wissen Sie, dass Sie ein Problem haben.

Wenn Sie ein startfähiges externes Laufwerk haben, kann ein Start von diesem Laufwerk aus helfen, Probleme zu isolieren, oder aber eine andere Umgebung zur Verfügung stellen wie z.B. eine andere Version von OS X.

T: Target Disk Mode — Was ist, wenn Sie mit Hilfe des Startup Managers vom Laufwerk eines anderen Macs starten wollen? Sie können die Macs über FireWire oder Thunderbolt miteinander verbinden und dann den anderen Mac in den Target Disk Mode versetzen, der ihn wie ein externes Laufwerk nutzen lässt. Halten Sie dazu auf dem anderen Mac die Taste **T** während des Startvorgangs, um in diesen Modus zu gelangen. Wenn einer der beiden Macs weder über FireWire noch über Thunderbolt verfügt, haben Sie kein Glück.

Außer für Problemlösungen kann der Target Disk Mode auch hilfreich sein, rasch viele Gigabytes an Dateien zu übertragen. Und wenn das Display Ihres Macs versagt, können Sie den Target Disk Mode nutzen, um Ihr Laufwerk als Startdisk für einen Mac mit funktionierendem Bildschirm zu benutzen.

Shift-Control-Option: SMC-Reset — Wenn Ihr Mac echt seltsames Verhalten an den Tag legt, kann es helfen, den System Management Controller (SMC) zurückzusetzen, der alle möglichen Dinge kontrolliert wie z.B. Batterien, die Tastatur-Hintergrundbeleuchtung und die Kühlungs-Ventilatoren. Apple listet all die Dinge auf, die ein SMC Reset reparieren kann.

Auf Desktop-Macs setzt man den SMC zurück, indem man das Stromkabel für 15 Sekunden abzieht, es wieder anschließt und den Mac nach weiteren 5 Sekunden einschaltet. Auf älteren Mac Notebooks kann man den SMC zurücksetzen, indem man die Batterie und das Stromkabel entfernt, den Einschaltknopf 5 Sekunden gedrückt hält, um die Kondensatoren zu entladen, dann die Batterie wieder einsetzt und den Mac wieder einschaltet.

Bei neueren Mac Notebooks, bei denen es nicht möglich ist, die Batterie zu entfernen, muss man diese Tastenkombination kennen: Shift-Control-Option, wobei man die Tasten auf der linken Seite der Tastatur benutzt. Schalten Sie Ihren Mac aus, schließen Sie das Netzkabel an, drücken Sie ⇧ctrl⌥ und dann den Einschaltknopf, während Sie diese Tasten immer noch gedrückt halten. Lassen Sie die Tasten dann los und drücken Sie den Einschaltknopf noch einmal, um den Mac mit frischen SMC-Einstellungen wieder hochzufahren.

Command-Option-P-R: NVRAM-Reset — Eine andere schnelle Reparaturmöglichkeit ist das Zurücksetzen des Non-Volatile Random Access Memory (NVRAM), was man durch Halten der Tasten Command-Option-P-R beim Starten des Macs erreicht. Der Start-Gong des Macs sollte dabei ein zweites Mal ertönen. Danach lassen Sie die Tasten los. Der Grund für den Gebrauch der Tasten P und R in dieser Tastenkombination ist, dass Apple diesen nicht-flüchtigen Speicher früher „PRAM" (Parameter-RAM) nannte.

Das NVRAM kontrolliert Dinge wie die Lautstärke der Lautsprecher, Bildschirmauflösung und die Auswahl des Startlaufwerks. Wie ein SMC-Reset kann ein NVRAM-Reset eine Reihe scheinbar zufälliger Probleme beheben.

Shift: Safe Mode — Wenn Ihr Mac sich während des Start-Prozesses aufhängt, kann ein Hochfahren im Safe Mode helfen festzustellen, was falsch läuft. Um den Safe Mode einzuleiten, halten Sie die Umschalttaste ⇧ während des Starts. Das bewirkt folgende Dinge:

- Überprüfung und Reparatur der Startup Disk
- Nur die wichtigsten Kernel-Erweiterungen werden geladen.
- Startobjekte werden ignoriert.
- Vom Benutzer installierte Zeichensätze werden deaktiviert.
- Alle System Cache Dateien werden gelöscht.

Einfach in den Safe Mode zu starten mag Ihr Problem bereits lösen, wenn es mit Korruption des Datenverzeichnisses oder durcheinander geratenen Cache-Dateien zu tun hatte. Wenn der Start im Safe Mode erfolgreich war, versuchen Sie anschließend sofort „normal" zu starten, und wenn auch das funktioniert, ist das Problem gelöst.

Wenn allerdings Ihr Mac zwar problemlos im Safe Mode startet, aber im übrigen weiterhin Probleme hat, haben Sie vielleicht ein Software-Problem mit etwas, was direkt beim Start geladen wird. Man kann darauf tippen, dass eine fremde Kernel-Erweiterung schuld ist; es kann aber auch ein defekter Zeichensatz sein. Schauen Sie sich in den diversen Library-Ordnern auf Ihrem Mac um.

Wenn Sie nur verhindern wollen, dass Startobjekte geladen werden, drücken Sie die Umschalttaste erst, wenn Sie den Login-Button im Login-Fenster anklicken oder sobald Sie den Fortschrittsbalken auf dem Startbildschirm sehen. Lassen Sie die Taste wieder los, sobald der Schreibtisch oder das Dock erscheint.

Command-R: Recovery — Jeder moderne Mac kann in einen speziellen Recovery Mode starten, der Werkzeuge für eine Reihe von Problemen bietet. Die System-Disk der meisten Macs enthält eine kleine Partition mit einer Minimal-Version von OS X, von der aus man den Mac starten kann, wenn man beim Start die Tasten Command-R gedrückt hält. Fehlt die Recovery Partition aus irgendeinem Grund, kann man die Recovery-Software auch aus dem Internet laden, indem man beim Start **Command-Option-R** gedrückt hält. Unnötig zu sagen: Die Internet Recovery zu laden braucht etwas länger; glücklicherweise wird dabei eine Zeit-Schätzung angezeigt.

Recovery bietet sieben Optionen:

- **Wiederherstellung aus einem Time Machine Backup:** Sie *haben* doch ein Time Machine Backup, nicht wahr?
- **OS X neu installieren:** Man braucht nicht die Platte zu löschen und bei Null anzufangen; diese Option installiert die aktuelle OS X Version neu über Ihre vorhandene Installation; das kann fehlende oder defekte Systemdateien reparieren. Wenn Sie die Internet Recovery benutzen, erhalten Sie stattdessen die OS X Version, mit der Ihr Mac im Originalzustand ausgeliefert wurde.
- **Online-Hilfe zu Rate ziehen:** Diese Option öffnet Safari, sodass Sie auf Apples Supportseiten nach Hilfe suchen können.
- **Festplatten-Dienstprogramm:** Ein Klick auf diesen Eintrag in der Liste bringt das Programm Disk Utility hervor, das Ihre Laufwerke überprüfen und reparieren kann. Wenn es unbedingt nötig ist, können Sie dieses Festplattendienstprogramm benutzen, um Ihre System-Disk zu löschen, worauf Sie dann Ihre Daten aus dem Time Machine Backup wiederherstellen können. (Sie *haben* doch so ein Backup, nicht wahr?)
- **Firmware-Password-Dienstprogramm:** Wählen Sie aus dem Menü Dienstprogramme > Firmware Password Dientsprogramm, um dieses Programm zu starten, mit dem Sie ein Firmware-Passwort setzen oder deaktivieren können. Sie möchten das Firmware-Passwort vielleicht nutzen, um „Find My Mac" sicherer zu machen (lesen Sie dazu „Disable Find My Mac by Resetting NVRAM", 22.07.2016).
- **Netzwerk-Dienstprogramm:** Ebenfalls verfügbar im Dienstprogramme-Menü, ermöglicht es das Network Utility, lokale und Internet-Verbindungen mit Werkzeugen wie Netstat, Ping, Traceroute u.a. zu prüfen. Es ist leichter anzuwenden, wenn der Mac nicht im Recovery Mode ist, aber es ist da, wenn Sie es brauchen.
- **Terminal:** Diejenigen, die sich in der Befehlszeilen-Umgebung wohler fühlen, können auch das Terminal aus dem Dienstprogramme-Menü heraus starten. Es ist eine verkleinerte Installation, der einige Unix-Werkzeuge fehlen mögen, die Sie gewohnt sind, aber man kann herum manövrieren, Dateien anschauen und Dinge löschen. Seien Sie vorsichtig!

D: Apple Diagnostics — Wenn nichts vom bisher Erwähnten Ihr Problem lösen konnte, leidet Ihr Mac vielleicht an einem Hardware-Problem. Halten Sie die Taste **D** beim Start, um Apple Hardware Test oder Apple Diagnostics zu öffnen.

Welches von beiden Sie bekommen, hängt vom Alter Ihres Macs ab; Macs, die vor Juni 2013 produziert wurden, haben den Apple Hardware Test, während jüngere Macs Apple Diagnostics haben. Beide Programme tun grundsätzlich dasselbe, aber der Apple Hardware Test ist ein echter Blick in die Vergangenheit — er sieht aus wie das alte klassische Mac OS (damals vor OS X)! Apple Diagnostics sieht viel eleganter aus und arbeitet mehr oder weniger automatisch, während man einen Button klicken muss, um Apple Hardware Test zu starten. Apple Hardware Test gibt einem die Wahlmöglichkeit eines erweiterten Tests, der viel länger braucht und in der Regel nicht nötig ist. Apple empfieht, alle externem Geräte abzukoppeln (außer Tastatur, Maus, Bildschirm und Ethernet-Kabel), bevor man die Tests beginnt.

Wenn Sie aus irgendeinem Grund nicht in diese Tests starten können, drücken Sie stattdessen **Option-D**, um einen Internet-basierten Hardware-Test zu laden.

Command-V: Verbose Mode — Hält man beim Start die Tasten Command-V gedrückt, versetzt das Ihren Mac in den verbose mode, den geschwätzigen Modus. Anstelle des geschmackvollen grauen Bildschirms sehen Sie jede einzelne Unix Systemmeldung, während Ihr Mac hochfährt. Der verbose mode kann nützlich sein, wenn man ein Unix-Experte ist; ansonsten ist er meist nur amüsant anzuschauen.

Command-S: Single-User Mode — Um noch einen Schritt über den *verbose mode* hinauszugehen, halten Sie Command-S während des Startvorgangs, was Ihren Mac in den *single-user mode* versetzt. Wenn der Mac fertig damit ist, all seine Unix-Meldungen während des Startvorgangs anzuzeigen, erhalten Sie einen Befehlszeilen-Prompt, so, als wären Sie im Terminal. So wie die Anwendung des Terminals aus der Recovery heraus ist der *single-user mode* meist nur dann nützlich, wenn Sie sich mit Unix auskennen. Manche Leute benutzen den *single-user mode*, um das Unix-Dienstprogramm fsck laufen zu lassen, obwohl es einfacher ist, in den *safe mode* zu starten oder das Festplattendienstprogramm für diesen Zweck zu benutzen.

Um den *single-user mode* wieder zu verlassen und den Startvorgang des Macs fortzusetzen, tippen Sie `exit` und drücken Return. Oder Sie tippen, um ganz von vorn zu starten, `reboot` und drücken Return.

Weder *single-user mode* noch *verbose mode* stehen zur Verfügung, wenn Sie ein Firmware-Passwort aktiviert haben.

C: Start von einem Wechsel-Medium — Wenn Sie die C-Taste beim Start halten, startet der Mac von einem wechselbaren Medium wie einer CD, DVD oder einem USB-Stick. Da Apple optische Laufwerke weitgehend von seinen Rechnern verbannt hat und physische Installations-Discs ein Ding der Vergangenheit sind, ist dieses Kürzel bei weitem nicht mehr so nützlich wie es einmal war. Die Optionstaste zu benutzen, um den Startup Manager aufzurufen, ist die bessere Option, weil Sie dann genau wissen, von welchem Laufwerk Sie starten.

Auswerfen, F12: Alle Wechsel-Medien auswerfen — Hier ist ein netter Trick: Wenn Sie beim Start die Auswerfen-Taste gedrückt halten (wenn Ihr Mac eine hat), oder F12 oder den Maus-Button oder den Trackpad-Button, wird der Mac alle entfernbaren Medien auswerfen. Wie das C-Kürzel ist diese Technik nicht mehr so nützlich wie damals, als dies die Standard-Methode war, um alle Datendisketten rasch auszuwerfen, aber sie ist es wert, sich daran zu erinnern, wenn Sie einmal an einem alten Mac arbeiten sollten.

N: NetBoot — Halten Sie die Taste **N** beim Start gedrückt, startet der Mac von einem verfügbaren NetBoot-Server. Hält man **Option-N**, startet das voreingestellte Boot Image auf einem NetBoot-Server.

Für diejenigen, die noch nie etwas von NetBoot gehört haben: Das ist eine Apple-Technologie in OS X Server, die es Macs ermöglicht, das Betriebssystem von einem Server im Netzwerk zu laden statt von einem lokalen Laufwerk. Große Netzwerke benutzen manchmal NetBoot, um sicherzustellen, dass jeder Mac im Netz ein und dieselbe, geprüfte Version des Betriebssystems verwendet. Wahrscheinlich aber müssen Sie sich keine Gedanken über NetBoot-Starts machen.

X: Startet OS X statt Classic — Zum Schluss noch die Taste **X**, die den Mac laut Apple dazu veranlasst, „von einem OS X Startup-Volume zu starten, wenn er sonst von einem Nicht-OS-X-Volume starten würde".

Dies ist ein Überbleibsel aus der Frühzeit von OS X, als man damit den Mac davon abzuhielt, in die Classic-Umgebung und mit MacOS 9 zu starten.

Umgekehrt sorgte die Taste **9** damals für einen Start in die Classic-Umgebung. *Das ist heutzutage natürlich nur noch als Anekdote interessant.*