Internetsicherheit 1×1

Täglich werden Webseiten gehackt, Passwörter ausgespäht, Identitäten gestohlen. Mit ein paar einfachen Tipps und Tricks kann man viele solcher Attacken auf die eigenen Online-Accounts vermeiden oder zumindest deutlich erschweren.
Alle hier vorgestellten Applikationen, Tools und Webseiten sind Präferenzen des Autors (@Tim_Steinbach) und sollen lediglich dazu dienen, generelle Strategien zur Vermeidung bzw. Erschwerung von Hacks und Identitätsdiebstahl darzustellen. Nichts und Niemand ist sicher vor solchen Angriffen, aber mit einigen Änderungen im täglichen Trott des Internets kann man bereits viel erreichen.

Übersicht

Passwortstärke

Die meisten Webseiten und Systeme im Internet basieren darauf, Benutzer durch Namen oder E-Mail Adresse und ein entsprechendes Passwort zu authentifizieren.
Das Problem ist, dass man Passwörter ständig eingeben muss. Also scheint es sinnvoll, sich die Passwörter einfach zu merken, sie kurz zu halten und am besten auch immer das selbe Passwort zu benutzen, dann kommt man nicht durcheinander.
Aber dies ist exakt, was man **nicht** tun sollte!

Am wichtigsten ist es, einige simple Regeln zu befolgen:

1. **Kein** Passwort sollte für mehr als eine Webseite verwendet werden
2. Passwörter sind **privat** und sollten **niemandem** mitgeteilt werden

3. Passwörter sollten **komplex** sein
4. Passwörter dürfen **nicht** aus Wörtern bestehen, die in einem Wörterbuch zu finden sind

Die erste Regel ist wichtig in Fällen, in denen eine Webseite gehackt wird (was praktisch ständig passiert) und ein Hacker Passwörter entschlüsselt. Hat man das selbe Passwort bei allen Webseiten, so kann der Hacker nun mit dem Passwort von einer einzigen Quelle in alle anderen Webseiten einloggen.
Regeln 3 und 4 erschweren das Hacken des Passworts. Wir gehen ein wenig auf diese beiden Regeln ein, bevor wir uns dem Problem des Generieren von starken Passwörtern und dem damit verbundenen Problem, dass man sich starke Passwörter in der Regel kaum bzw. gar nicht merken kann.

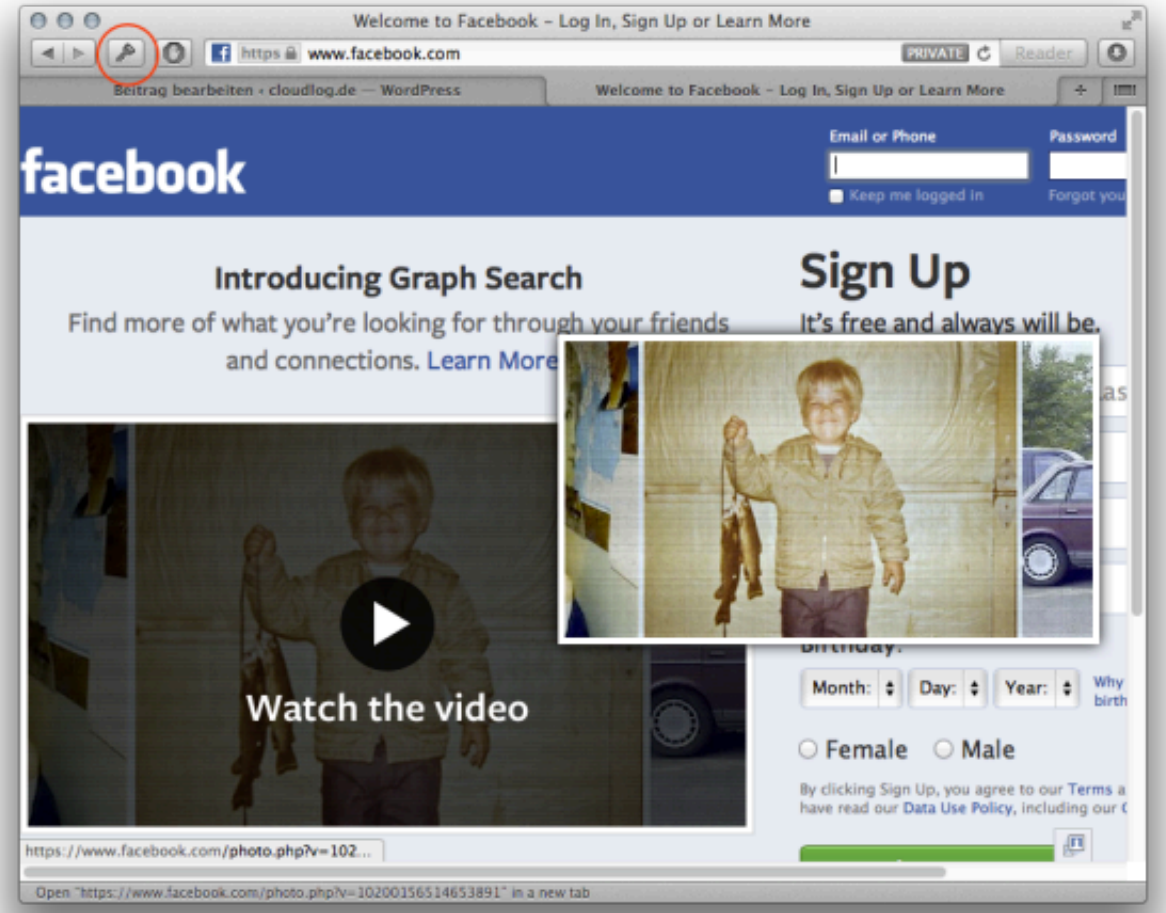
Gute & schlechte Passwörter

Folgt man den Richtlinien von Microsoft oder Google, sollte ein gutes Passwort wenigstens acht(8) Zeichen enthalten. *Je mehr, desto besser!*
Außerdem ist es wichtig, kein einfach lesbares Passwort zu haben, z.B. ein Wort, das in einem Wörterbuch zu finden ist. Genauso sind Geburtstage, Namen und Kombinationen aus den Dreien vollkommen unbrauchbar als Passwörter.
Das zufällige Aneinanderreihen von kleinen und großen Buchstaben sowie Sonderzeichen und Ziffern ist essentiell für die Sicherheit eines Passwortes, denn man sollte verhindern, dass es weder erraten werden kann, noch ein Computer alle Kombinationen ausprobieren kann.

1Password

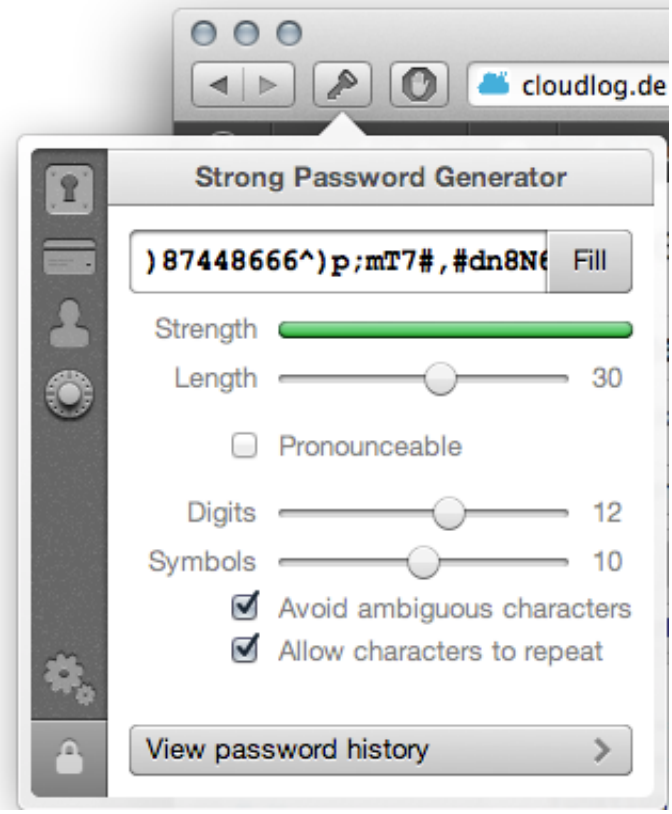
1Password ist eine Applikation des kanadisches Softwarehauses Agilebits. Es bietet verschiedene Funktionalitäten, die Passwörter generell stärker machen sollen und gleichzeitig dabei helfen, dass man seine Passwörter nie wieder vergisst.
1Password speichert alle Passwörter sicher in einer Container-Datei, welche mit einem Masterpasswort geschützt ist. Dieses Masterpasswort ist das **einzige**, das man sich nun noch merken muss. Gleichzeitig sollte es jedoch offensichtlich nicht zu einfach zu erraten sein, denn dann hat ein Angreifer gleich Zugriff auf eine Sammlung von Passwör-

tern zu diversen Webseiten. Aber es ist logischerweise deutlich einfacher und sicherer, sich ein einzelnes starkes Passwort zu merken als eins zu jeder Webseite.



1Password im Browser

Für Firefox, Chrome und Safari gibt es jeweils eine Erweiterung, die 1Password direkt in den Browser integriert, sodass der Zugriff auf Passwörter möglich ist, ohne die eigentliche Applikation zu öffnen.
Gleichzeitig gibt es ein kleines Tool zur Passwortgenerierung. So muss man sich starke Passwörter nicht mehr ausdenken, sondern kann wirklich zufällige Kombinationen von Zeichen benutzen. 1Password ermöglicht es, die Passwortlänge und Anzahl der Ziffern bzw. Sonderzeichen im Passwort festzulegen. Dies ist sinnvoll bei Webseiten, die die Passwortlänge begrenzen.



Passwortgenerator

Um den Workflow beim Surfen noch zu beschleunigen, bietet 1P die Tastenkombination ⌘ + \ (Mac), welche automatisch ein Loginformular auf der aktuellen Webseite auszufüllen versucht. Ist die Auswahl nicht eindeutig (es gibt keine oder multiple gespeicherte Logindaten), so wird eine Liste aller passenden Einträge angezeigt.

1Password gibt es für OSX, iOS und Windows. Die Containerdatei, welche die Logindaten enthält, kann per Dropbox oder iCloud zwischen verschiedenen Geräten synchronisiert werden.

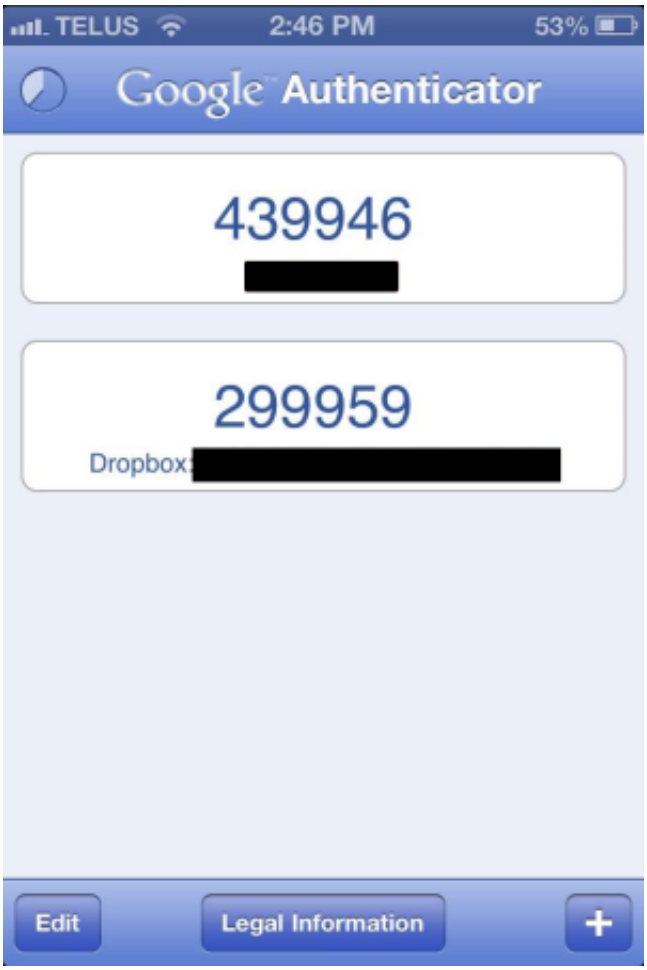
Alternativ zu 1Password kann die OpenSource Lösung KeePass erwähnt werden. KeePass enthält die wesentlichen Features, die hier für 1Password exemplarisch dargestellt wurden.

OAuth

OAuth ist ein Authorisierungsprinzip, welches derzeit von vielen Webseiten genutzt wird. Immer, wenn man sich auf einer Webseite anmelden kann, indem man seinen Facebook, Twitter, Google oder sonstigen Account benutzt, dann geschieht diese Authorisierung per OAuth. Anstatt einen neuen Account mit einer Webseite zu erstellen, benutzt man so einen bereits existierenden Account.
OAuth, solange es korrekt implementiert worden ist, gilt derzeit als relativ sicher. Es hat jedoch ein gravierendes Problem, welches nicht direkt auf OAuth, sondern auf die Idee an sich zurückzuführen ist: Wird der Service Provider (z.B. Twitter), der OAuth zur Verfügung stellt, von Angreifern erfolgreich attackiert, so haben die Angreifer nicht nur Zugriff auf die Twitterkonten, sondern gleichzeitig auf alle via OAuth authorisierten Webseiten dieser Konten.
Wer also beispielsweise Facebook nutzt, um sich bei SPIEGEL ONLINE anzumelden, sollte sich sicher sein, dass sein Facebookpasswort sicher ist!

2-Step Authentication

In den letzten Monaten haben sich langsam Betreiber wichtiger Dienste (u.a. manche der genannten OAuth Service Provider) dazu entschlossen, sich nicht nur auf Passwörter zu verlassen. Dies wurde teilweise durch großflächige Angriffe auf die Services notwendig, denn allein im Jahr 2012 gab es mehrere erfolgreiche Angriffe, die viele 100.000 Benutzerdaten kompromittiert haben.
Facebook, Dropbox und Google erlauben es Benutzern nun, die sog. 2-Step Authentication einzuschalten. Das bedeutet, dass man neben seinem Passwort noch einen weiteren Code benötigt, der durch ein Tool erzeugt wird und sich in der Regel alle 30-60 Sekunden ändert. Bei Facebook kann man sich diesen Code entweder durch die mobile Applikation erstellen oder per SMS zusenden lassen.
Dropbox und Google nutzen den Google Authenticator, der für iOS, Android und Blackberry verfügbar ist.



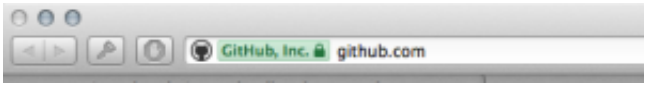
Google Authenticator

Der große Vorteil einer solchen Lösung ist, dass ein Hacker, der das Passwort eines Accounts herausfindet, ohne physikalischen Zugriff auf das Smartphone mit der passenden Applikation sich noch immer nicht einloggen kann.
Für Benutzerkonten mit persönlichen Daten, wie beispielsweise soziale Netzwerke und E-Mail-Konten, ist 2-Step Authentication sehr empfehlenswert, um Identitätsdiebstahl zu verhindern und seine Privatsphäre zu schützen.

HTTPS

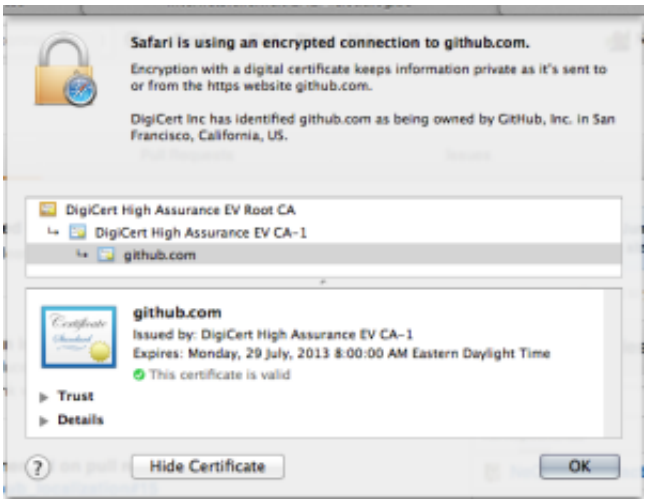
In der Regel werden Daten im Internet praktisch im Klartext übertragen und jede Person kann mitlesen, was in seinem Netzwerk passiert. Dies wird besonders kritisch, wenn man sich in einem kostenlosen WLAN im Restaurant oder in der Universität befindet und potentiell hun-

derte Personen sehen können, auf welcher Webseite man gerade etwas macht. Noch kritischer wird es aber, wenn Benutzerdaten auf die gleiche Art und Weise übertragen werden. Plötzlich haben all diese hunderte potentiellen Lauscher den Namen und das Passwort direkt vor sich auf dem Bildschirm!
Genau dies wird verhindert, wenn Webseiten die Verbindung per SSL verschlüsseln. Wenn dies der Fall ist, so zeigt der Browser dies in der Regel dadurch an, dass die URL mit *https://* beginnt. Zusätzlich haben moderne Browser eine farbliche Markierung.



Webseite mit SSL

SSL basiert auf asynchroner Verschlüsselung, der öffentliche Schlüssel wird in Zertifikaten festgehalten. Diese Zertifikate kann man sich anzeigen lassen. Wie genau dies funktioniert, hängt stark vom verwendeten Browser ab. Die Auflistung der Informationen zu einem Zertifikat hingegen ist in allen Browsern ähnlich.



SSL Zertifikat

Fazit

Starke Passwörter sind wichtiger als je zuvor. Hacker entwickeln immer bessere Tools, um Passwörter zu knacken. Sollte der eigene Account einmal gestohlen werden, kann der Schaden dadurch begrenzt werden, dass man für jede Webseite ein eigenes Passwort benutzt hat.
Es gibt Applikationen, die für jeden Internetbenutzer zur Grundausstattung gehören sollten und mit der Passwortverwaltung und -generierung helfen.
Zusätzliche Sicherheit bieten 2-Step Systeme, die ebenfalls ein One Time Password (OTP) abfragen. Diese Systeme verhindern, dass ein Konto gestohlen werden kann, wenn ein Hacker das Passwort erraten oder anderweitig herausgefunden hat. Der erhöhte Aufwand beim Einloggen (Eintippen des OTP) ist die verbesserte Sicherheit definitiv wert.
Bei Webseiten mit sensiblen Informationen sollte man zudem darauf achten, dass gültige SSL-Zertifikate verwendet werden, damit andere Netzwerkbenutzer die Kommunikation mit den Webseiten nicht einfach mitlesen können.