Sichere Passwörter
und deren Management

Tobias Diekershoff

Version 1.3, 17.01.2019, FSFE Berlin Supporter Treffen vom 10.01.2019

Inhalt

Das Jahr 2019 ist noch jung, da wird die Republik erschüttert. Erschüttert von einem Datenskandal sonder gleichen. Zur ansonsten ruhigen und besinnlichen Jahresendzeit 2018 gab es einem Hackerangriff auf Hunderte Politiker (tagesschau.de am 4.1.2019). So wirklich Genaues wusste man nichts, aber es herrscht Empörung nach der Cyberattacke (tagesschau.de, 4.1.2019). Bis der Fall dann am Dienstag geklärt war Tatverdächtiger nennt Verärgerung über Politiker als Motiv (RBB24, 8.1.2019). Oder halt auch nicht. Es bleibt *spannend*, denn wie das Magazin Kontraste vom RBB herausgefunden haben will (vergl. RBB24, 16.1.2019) soll der Geständige nicht über das nötige Wissen verfügen.

Darum soll es aber hier gar nicht gehen. Vielmehr will ich einen kleinen Aspekt der Digitalen Selbstverteidigung (Electronic Frontiers Foundation, EFF) aufgreifen: sichere Passwörter (EFF) und deren Management.

Über den Verfasser

Tobias ist FLOSS Enthusiast aus Berlin und Nutzer von GNU/Linux seit Mitte der 1990er. Er ist Fellow der Free Software Foundation Europe und Mitentwickler beim Friendica Projekt.

Fragen oder Hinweise auf Fehler bzw. Unklarheiten können an tobias.diekershoff@gmx.net gerichtet werden. Gerne auch mit GNUPG signiert und verschlüsselt. Mein Key hört auf die ID `0x25FE376FF17694A1` und hat folgenden Fingerabdruck:

```
23EE F484 FDF8 291C BA09
A406 25FE 376F F176 94A1
```

Das Handout und die Folien des Vortrags können gerne weiter gegeben werden. Da sie Bilder vom XKCD beinhalten und diese von Randall Munroe unter CC-BY-NC 2.5 gestellt wurden, gilt auch für die Folien und das Handout die CC-BY-NC Lizenz in der Version 2.5.

Was war geschehen?

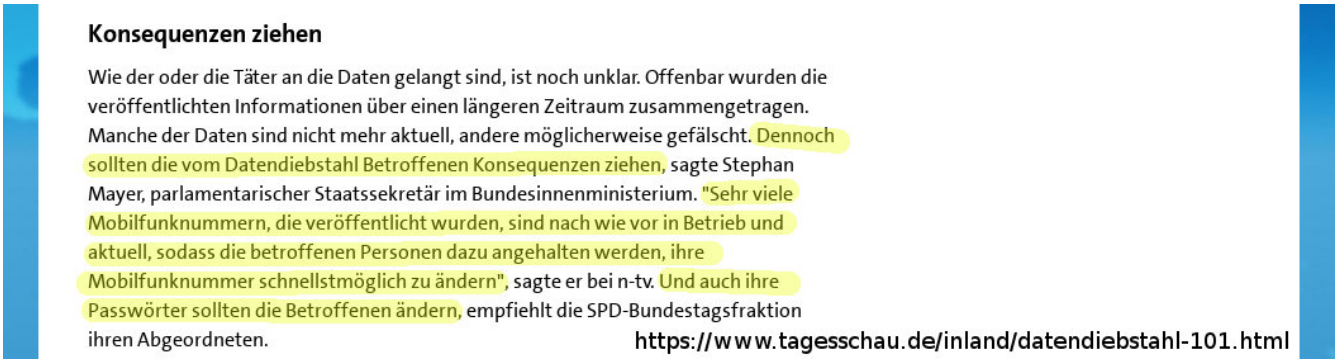
Tagespresse und Politiker überschlugen sich da ein wenig. Von großen Angriffen auf die Demokratie war da die Rede und einem totalen Versagen der (Cyber-)Sicherheit in Deutschland. Irgendwie hatte ich das Gefühl, die Welt steht vor dem Abgrund.

Da hatte jemand persönliche Daten gesammelt und diese dann veröffentlicht. Inzwischen ist anscheinend klar wer es war (RBB24 vom 8.1.2019), er war wohl verärgert über öffentliche Äußerungen. Im Englischen nennt sich das ganze übrigens Doxing (von Docs für Dokumente). Bei uns ist das *Ausspähen von Daten*; ist bei Erwachsenen ein Strafmaß von bis zu drei Jahren plus Geldstrafe vorgesehen, sowie der Tatbestand der *Datenhehlerei* mit gleichem Strafmaß (vergl. obiger RBB24 Artikel).

An sich egal was genau da jetzt passiert ist. Zu solchen Leaks, Daten abgriffen, *Einbrüchen* wird es

immer wieder kommen. Deswegen denke ich sollte man versuchen die Auswirkungen eines Passwort Leaks so klein wie möglich zu halten. Passwörter sind da ein Teil der Gleichung.

Bin ich auch betroffen?



Konsequenzen ziehen

Wie der oder die Täter an die Daten gelangt sind, ist noch unklar. Offenbar wurden die veröffentlichten Informationen über einen längeren Zeitraum zusammengetragen. Manche der Daten sind nicht mehr aktuell, andere möglicherweise gefälscht. Dennoch sollten die vom Datendiebstahl Betroffenen Konsequenzen ziehen, sagte Stephan Mayer, parlamentarischer Staatssekretär im Bundesinnenministerium. "Sehr viele Mobilfunknummern, die veröffentlicht wurden, sind nach wie vor in Betrieb und aktuell, sodass die betroffenen Personen dazu angehalten werden, ihre Mobilfunknummer schnellstmöglich zu ändern", sagte er bei n-tv. Und auch ihre Passwörter sollten die Betroffenen ändern, empfiehlt die SPD-Bundestagsfraktion ihren Abgeordneten.

https://www.tagesschau.de/inland/datendiebstahl-101.html

Abbildung 1. Betroffene sollten Passwörter und Telefonnummern ändern (Screenshot tagesschau.de)

Stellt sich also die Frage, bin *ich* auch betroffen. Sind meine Zugangsdaten und persönlichen Informationen online in Leaks enthalten?

Und die Antwort ist: *wahrscheinlich ja*. Und wenn jetzt noch nicht, dann wahrscheinlich demnächst. Leaks können jedem passieren. Eine Liste von Leaks habe ich auf haveibeenpwned.com gefunden. An *Yahoo!* erinnern wir uns ja vielleicht noch vom letzten Jahr, aber da stehen dann auch so Namen wie *Adobe*, *Minecraft* und *Dropbox*. Andere Listen (vergl. die Webseite des HPI Identity Leak Checkers) enthalten noch so illustre Namen wie *Hotmail*, *gmail*, *yandex* uvm..

Statistisch werden jeden Tag knapp eine Millionen E-Mail Adressen / Passwort Paare von Online-Diensten geleakt, d.h. Zugänglich gemacht. Da kann man sich jetzt schnell ausrechnen, bei 7 Milliarden Menschen auf dem Planeten Erde dauert es 7000 Tage bis ein Account eines jeden Menschen öffentlich wird. Selbst die Accounts der Babies. 7000 Tage sind 20 Jahre. Nun haben die meisten Menschen aber mehr als nur einen Account. Ich hab kurz überschlagen, mit meinen Social-Media-Accounts, E-Mails, Foren, Online-Händlern bin ich eher so bei 20 bis 30. Macht also für mich statistisch ein Leak pro Jahr.

Es gibt diverse Dienste bei denen man überprüfen lassen kann, ob seine E-Mail Adresse in einem der bekannten Leaks enthalten gewesen ist. Ob man denen Vertrauen schenkt ist bei jedem einzelnen so eine Sache, die man mit sich selbst ausmachen muss. Dem oben genannten *haveibeenpwned* scheint vertrauenswürdig zu sein (vergl. EN Wikipedia) ich habe mich dennoch für eine Alternative aus Deutschland entschieden.

Unter anderem bietet das Hasso Plattner Institut der Universität Potsdam auch so einen solchen Dienst unter sec.hpi.uni-potsdam.de/ilc. Das HPI steht irgendwie höher auf meiner Vertrauensleiter. Darum habe ich bei denen mal den Selbsttest gemacht.

Abbildung 2. Screenshot des Identity Leak Checker vom HPI

Also E-Mail Adresse(n) eingegeben und auf die Ergebnisse eine Minute warten.

In der Antwort Mail mit den Ergebnissen des Checks steht dann entweder drin

- Glückwunsch uns sind keine Leaks zu dieser E-Mail Adresse bekannt, oder
- es gibt eine Auflistung der betroffenen Dienste mit einer Aufstellung darüber welche persönlichen Daten in dem Leak betroffen sind.

So *wirklich* betroffen bin ich wohl nicht. Zumindest hatten die nur einen Datensatz mit meiner E-Mail Adresse. Und bei dem Dienst im Netz hatte ich ein zufällig generiertes Passwort verwendet.

Aber das heißt ja nicht, dass es nicht noch andere Listen gibt. Deshalb, selbst wenn keine Datensätze gefunden werden, lieber sorgsam mit Passwörtern umgehen.

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

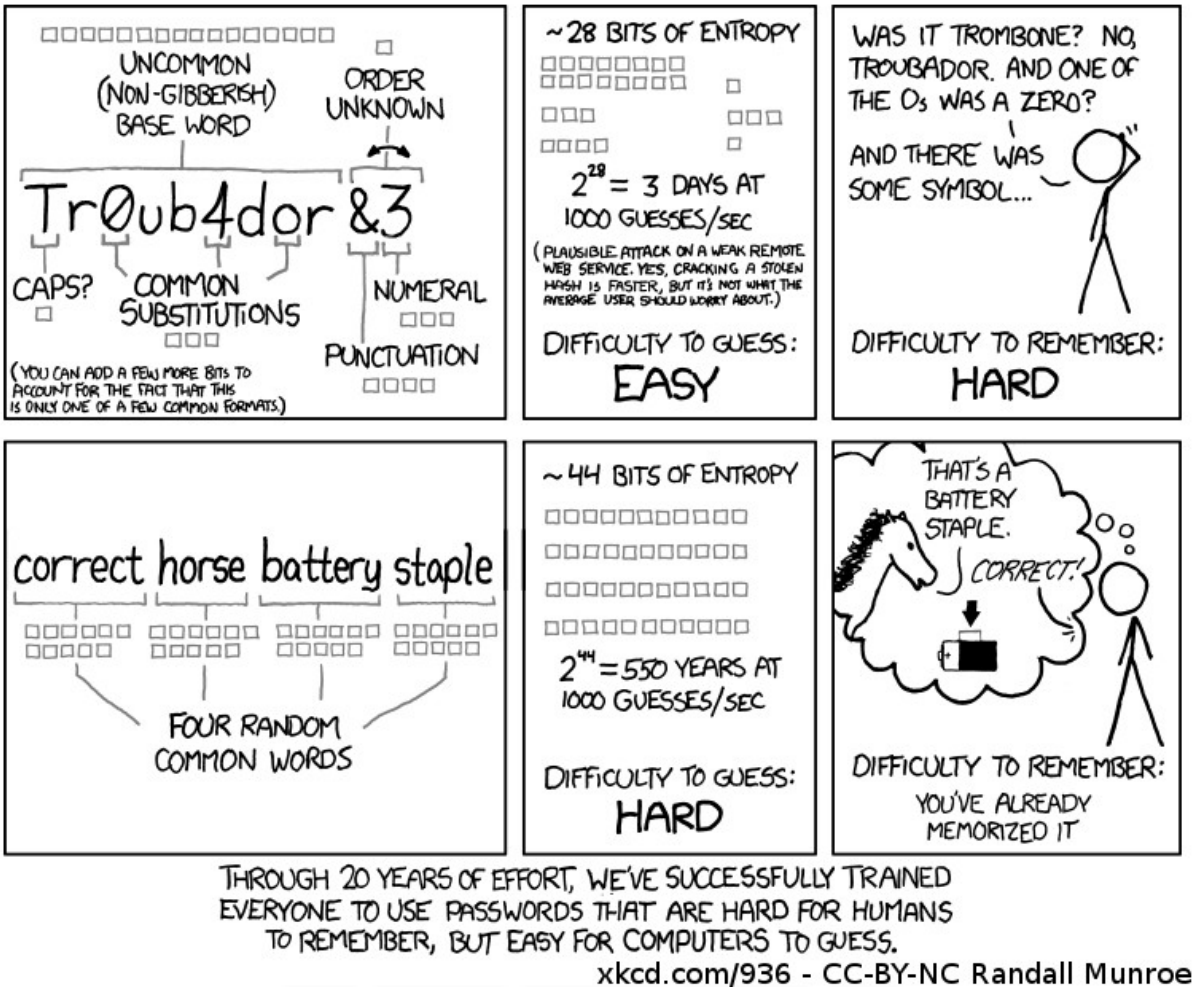
ACHTUNG

Ihre E-Mail Adresse taucht in mindestens einer gestohlenen und unrechtmaessig veroeffentlichten Identitaetsdatenbank (so genannter Identity Leak) auf. Folgende sensible Informationen stehen im Zusammenhang mit Ihrer E-Mail-Adresse:
tobias.diekershoff@gmx.net

Betroffener Dienst:	kickstarter.com
Datum:	Feb. 2014
Verifiziert:	Ja
Betroffene Nutzer:	5.174.845
Passwort:	Betroffen
Vor- und Zuname:	-

Abbildung 3. Ergebnis E-Mail vom HPI mit der Zusammenfassung der betroffenen Daten

Sichere Passwörter erzeugen



Einige Dinge die man unbedingt **vermeiden** sollte:

- Nicht einfach Wörter auf Wörterbüchern verwenden.
- Auch nicht zwei Mal hinter einander geschrieben.
- Oder gefolgt von einer Zahl.
- Keine Namen, Dinge oder Zahlen aus dem persönlichen Umfeld verwenden. Namen von Haustieren, Autokennzeichen, Telefonnummern, Geburtstage usw..
- Einfache Sequenzen und Wiederholungen von Zeichen.

Zufallsgenerator

Eine Schwachstelle von Passwörter ist, dass wir sie uns merken müssen. Das führt bei vielen Menschen dazu, wohl bekannte Begriffe oder Zahlen zu verwenden.

Also den Namen des Haustiers mit dem Geburtsdatum des Partners kombiniert. Wenn dich ein Angreifer kennt, dann kann er solche Passwörter allerdings genauso relativ leicht erraten.

Um das zu umgehen, kann man den Zufall ins Spiel bringen. Und zwar auf unterschiedlichste Arten.

Zum Beispiel können die meisten Passwort Manager zufällige Passwörter generieren, die den gängigen Kriterien für starke Passwörter entsprechen. Also lange Zeichenketten die Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Oder man verwendet andere Spezialprogramme wie `pwgen` auf der Kommandozeile unter Linux. Oder man greift zu einem guten, dicken Buch, schlägt vier Seiten auf und notiert sich jeweils das letzte Wort der dritten Zeile auf der Seite.

Ein kleines Beispiel mit dem Kommandozeilen Tool `pwgen` unter Linux. Die Parameter `-B` verhindern das ähnliche Zeichen in einem Passwort verwendet werden (`1` und `l`), das macht es für Menschen einfacher, nimmt dem Passwort aber Variationen, macht es damit prinzipiell einfacher zu erraten. Der Parameter `-N 10` sorgt dafür, dass gleich 10 Passwörter generiert werden. Zu guter Letzt verlangen wir mit der abschließenden `20` das Erzeugen von eben 20 Zeichen langen Passwörtern.

```
$> pwgen -B -N 10 20
```

Das Ergebnis ist dann eine Liste mit 10 Passwörtern von denen man sich eines aussuchen kann.

```
eesh9ea3PhaMeich9ohn chap4uHeiw3see4ei4sh shothu3Ahneo3jeiFee4
ohzingiqu4UkaeThai3x aevoosh9eoquohc7eChu ienieshoo7Uopai4xah9
gi4ieyieNgook3bahjua ietoo7chobie9aeno7oo ahgeeLeimeiph9ahwagu
aeraquai9aev4Va9phie
```

Die sind für Zufallspasswörter relativ gut zu merken. Andere Optionen, oder Generatoren, und die generierten Passwörter werden komplexer und weniger gut zu merken. Wobei, merkbar müssen die Zufallspasswörter auch gar nicht sein, wenn man sie in Passwort Managern gespeichert hat. Dazu später mehr.

Also werfen wir mal auf ein Zufallsverfahren einen Blick, bei dem leichter merkbare Passwörter

erzeugt werden.

Würfeln

Man kann auch den Würfel entscheiden lassen. Und das Ergebnis der Würfel mit Worten kombinieren, die dann das Passwort bilden. Im Internet gibt es dazu diverse Wortlisten, die verschiedene Würfelanweisungen mit Wörtern verknüpfen.

Mit einer solchen Liste an der Hand *würfelt* man einfach ein paar Worte aus, stellt die in einer beliebigen Reihenfolge hintereinander und erhält ein relativ einfach zu merkendes Passwort. Nach Bedarf können noch Zahlen und Sonderzeichen angefügt werden.

Die EFF hat z.B. solche Listen auf ihrer Homepage:

- EFF Dice-Generated Passphrases
- 20-Sided Dice and Fandom-Inspired Wordlists

Nehmen wir einfach mal die Game of Thrones-Liste. Für diese Liste will die EFF je drei Würfe eines zwanzig Seitigen Würfels (W20, oder denkt euch drei Zahlen zwischen 1 und 20 aus) pro Wort. Wir würfeln uns vier Wörter aus der Liste. Und garnieren mit zwei Sonderzeichen.

```
18-5-5 lordship      2-6-5 talking
13-7-9 night      17-20-11 explodes
```

lordship talking night explodes geht auch, ich persönlich finde aber *talking night; lordship explodes!* lustiger und irgendwie passt das auch mehr zu Game of Thrones. Also ist das für mich wahrscheinlich einfacher zu merken. Und die Satzzeichen garnieren die Wörter dann auch noch fast sinnvoll.

talking night; lordship explodes!

Anfangsbuchstaben

Wenn auch diese Passwörter zu schlecht zu merken sind, vielleicht hilft dann die folgende Methode. Man merkt sich einen Satz. Ein Zitat oder ähnlich vertrautes. Und dann nimmt man nicht den ganzen Satz als Passwort, sondern die Anfangsbuchstaben der einzelnen Wörter und Satzzeichen wie sie vorkommen.

Ein Beispiel:

> Der Weltraum, unendliche Weiten. Wir schreiben das Jahr 2200

von diesem Satz aus dem Intro einer bekannten TV-Serie, von daher eventuell eher ungeeignet für bekennende Star Trek Fans, ergibt sich das Passwort `DW,uW. WsdJ2200`. 14 Zeichen lang und beinhaltet Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Und man kann es sich einfach merken, indem man bei der Passwort-Eingabe den Satz im Kopf aufsagt und die ersten Buchstaben tippt.

So, jetzt haben wir also ein *gutes* Passwort. Aber *wie gut* ist es eigentlich?

Wie gut ist mein Passwort?

Gute Frage. Sollte es unter den am häufigst verwendeten Passwörter sein, ist es definitiv nicht gut. Das folgende Diagramm stammt von der Statistik-Seite des HPI Identity Leak Checker.

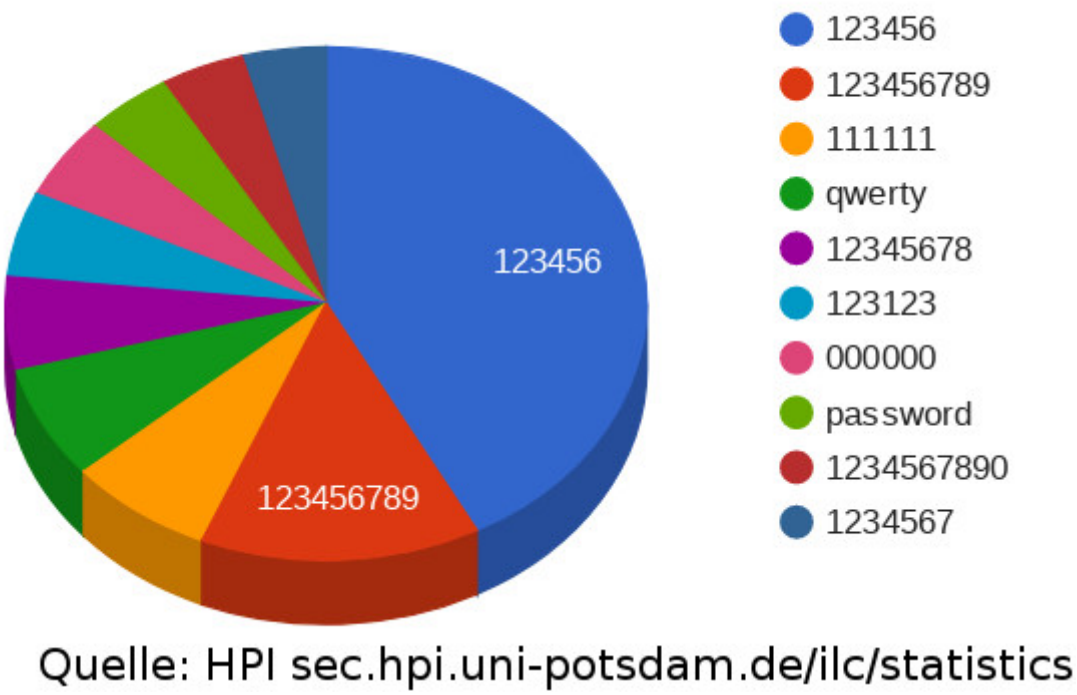


Abbildung 4. Die am häufigsten verwendeten Passwörter

Um zu überprüfen wie *gut* ein Passwort ist kann man z.B. den online Dienst howsecureismypassword.net verwenden. Da muss man ja nicht sein echtes Passwort eingeben, aber das Schema kann man ja überprüfen. Getestet wird wie lange ein Angreifer mit einer Milliarde Rate-Versuchen pro Sekunde braucht um auf das Passwort zu kommen (Brute-Force). Außerdem werden die 10.000 häufigsten Passwörter (aus bekannten Leaks) getestet und einige andere Tests wie sich wiederholende Wörter, Zahlen folgen auf Wörter. Verlasst euch nicht auf die Zahlen die der Tester da ausgibt. Aber ein *Gefühl* für die Güte des Passworts gibt das ja dennoch.

Testen wir zunächst einmal das am häufigsten verwendete Passwort `123456`. *Ja, wirklich*, es hat inzwischen sogar das *password* als Passwort abgelöst. (vergl. Wikipedia EN)

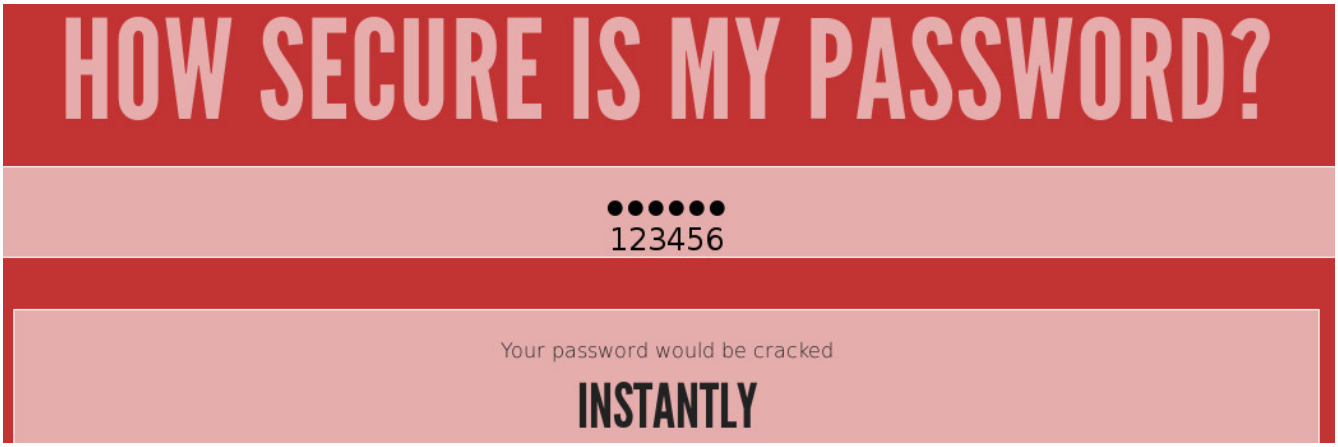


Abbildung 5. Bewertung des Passworts `123456` durch howsecureismypassword.net (Screenshot)

Ein anderer Versuch. *I love Free Software* etwas verfremdet geschrieben als `I <3 Free_Software`. Scheint noch akzeptabel zu sein; nur benutzt es jetzt nicht alle. Es ist deutlich länger, beinhaltet Gruß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Und es lässt sich noch relativ einfach merken. Allerdings ist es ggf. ein sehr naheliegendes Passwort.

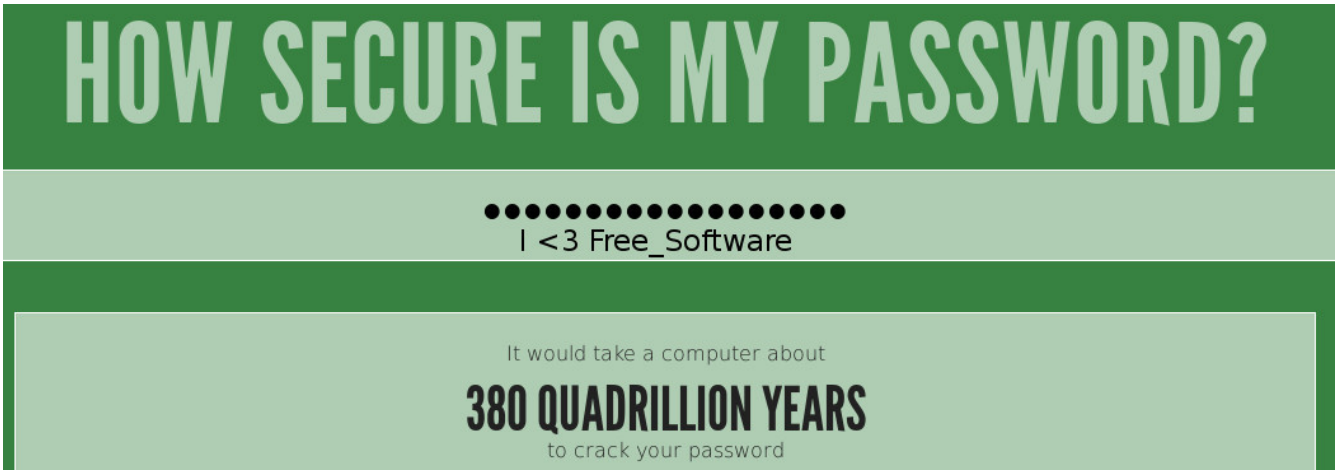


Abbildung 6. Bewertung des Passworts `I <3 Free_Software` durch howsecureismypassword.net (Screenshot)

Mit dem Tool kann man einfach mal spielen. Einfach mal Passwörter eingeben und zu sehen wie sich die Einschätzung des Passworts ändert wenn

- es länger wird
- unterschiedliche Zeichenklassen verwendet werden

und so.

Good Practise

Jetzt wo wir wissen wie man gute, starke Passwörter erstellt. *Wie geht man mit ihnen um?*

Die gängigen Tipps für Passwörter für Dienste/Seiten im Internet lauten:

- starke Passwörter verwenden
- **niemals** die gleichen Passwörter verwenden
- *regelmäßig* Passwörter ändern

- Sicherheits-Fragen *missbrauchen*
- Zwei-Faktor-Authentifizierung

und das kann ganz schön anstrengend werden.

Starke Passwörter tendieren dazu komplex zu sein. Und wenn man sich für viele Seiten die Passwörter merken muss, hat man entweder ein gutes Gedächtnis, ein einfaches Schema für die Passwörter oder kleine Helferlein.

Passwörter nicht wieder verwenden versteht sich von selbst. Wenn dann eine Nutzername (E-Mail) / Passwort Kombination *abhanden* kommt, dann ist der Schaden eher gering. Der Angreifer, und alle anderen die an dieses Passwort kommen, kennen dann nur das Passwort für den einen Dienst. Außerdem muss dann nur ein Passwort geändert werden, wenn das Leak bekannt wird, und nicht bei allen Accounts.

Regelmäßig ist ein schönes Wort. Meistens lese ich immer nur dieses eine Wort, aber keine genauere Angabe. Letztlich ist es etwas, das jeder für sich selbst entscheiden muss. Eine Abwägung zwischen Aufwand und Nutzen. Außerdem ist die Frage, wie sinnvoll es ist. Insbesondere wenn man lange, zufällig generiert Passwörter verwendet (vergl. Heise Wechselwahn). Wichtig ist auf jeden Fall, wenn der Betreiber einer Seite sagt, dass Daten abhanden gekommen sind **auf jeden Fall** das Passwort schnellst möglich ändern. Oder wenn man den Eindruck hat, dass da *Jemand anderes* auf den eigenen Account Zugriff hat.

Sicherheitsfragen sind toll. Besonders weil sie meist nach Dingen fragen, die *einfach* zu recherchieren sind. Deswegen einfach mal *falsch* beantworten. Meine Klassenlehrerin in der Grundschule? Der *Terminator 1000*! Alternativ kann man dann natürlich auch einfach ein Zufallspasswort rein werfen und gut ist.

Zwei-Faktor-Authentifizierung (2FA) ist auch ein schönes Mittel um *wichtige* Nutzerkonten weiter abzusichern. Dabei braucht man neben dem Nutzernamen und Passwort noch einen zweiten Faktor. Der sollte auf einem separaten Gerät, z.B. das Smartphone, erzeugt werden. Damit wird es noch etwas unwahrscheinlicher, dass ein Leak katastrophale Auswirkungen hat. Meist ist, z.B. das Smartphone, ja nicht in online verfügbaren Datensätzen enthalten. 2FA birgt aber auch die Gefahr, dass man den zweiten Faktor verliert und dann nicht mehr an das Nutzerkonto ran kommt. Trotzdem denke ich, wenn ein Dienst 2FA anbietet ist es sinnvoll sich gut zu überlegen, warum man es nicht einsetzen will.

Passwörter Verwalten

Sei es drum, wir haben jetzt gute Passwörter für all unsere Online-Dienste und wechseln sie einmal im Jahr. Wie merken wir uns jetzt die Passwörter. Eine mögliche Antwort ist einen *Passwort Manager* zu verwenden, quasi eine digitale Zettelsammlung mit ein paar zusätzlichen Features. Passwort Manager gibt es in etwa so viele wie Sand am Meer. Und die Auswahl beruht auf vielen Kriterien und persönlichen Vorlieben.

Soll heißen, nur weil ich bei KeePass gelandet bin, ist dass der ultimative beste Passwort Manager für **deinen Gebrauch**.

Und man sollte nicht vergessen, dass die Verwendung eines Passwort Managers auch wieder neue Probleme schafft. Dazu später etwas mehr.

Zunächst einmal die Frage klären, welchen Passwort Manager verwenden wir.

Welchen nehmen???

Wenn man sich mal entschlossen hat einen Passwort Manager zu verwenden stellt sich die Fragen *welchen denn*? Online-Dienste und Offline-Programme. Auf welchen Plattformen und welchen unterschiedlichen Betriebssystemen will man auf die Passwörter zugreifen. Desktop Programm oder eines auf der Kommandozeile?

In der (englischen) Wikipedia gibt es eine Liste von Passwort Managern. Die kann man als Ausgangspunkt der Recherche nehmen.

Meine persönlichen Kriterien waren damals

- Ich will die Daten bei mir haben. Also kein Cloud-Dienst.
- Die Datenbank muss mit einem Passwort gesichert sein.
- Der Passwort Manager muss Freie Software sein.

Der Aspekt Freier Software ist *mir* dabei sehr wichtig. Eine der Freiheiten ist, das sich jeder den Programmcode ansehen und ihn analysieren kann. Gerade bei sicherheitsrelevanter Software möchte ich mich nicht darauf verlassen, dass der Hersteller beschwichtigt und beteuert, dass die Software sicher ist. Da sollen bitte viele *Experten*, ohne Verschwiegenheitsklauseln, drauf gucken können um Schwachstellen zu beseitigen.

KeePass

Meine Wahl viel *damals* auf das Programm KeePass2, welches unter der Freien Software Lizenz *GNU GPLv2 or later*. Es ist verfügbar für die gängigen Betriebssysteme (Android, iOS, Linux, Windows). Und es erfüllt meine Anforderungen.

- die Passwort Datenbank ist AES/Rijndael oder ChaCha20 verschlüsselt
- es sind nicht nur die Passwörter verschlüsselt, sondern die gesamte Datenbank
- das Masterpasswort ist mit einem sicheren Hash (sha-256) gespeichert
- es unterstützt die Verwendung von mehreren Passwort Datenbankdateien
- KeePass ist *portable*, d.h. ich kann es auf meinem USB Stick mit mir herum tragen
- die Passwörter *können* in Gruppen sortiert werden
- Einträge können geändert werden. Beim Ändern kann man Zufallspasswörter generieren. Die Stärke des Passworts wird direkt beim Erzeugen angezeigt.
- Passwörter bleiben nur kurz im Zwischenspeicher beim Copy&Paste.
- Wenn neue Passwörter eingegeben werden, dann wird gleich angedeutet wie gut die sind.
- KeePass kann zufällige Passwörter erzeugen.

Wenn man die Passwort Datenbank öffnet, wird man zunächst nach dem Master Passwort gefragt. Oder kann den *Key File* angeben. Ich habe mich für ein Master Passwort entschieden.

Abbildung 7. KeePass Dialog zum Entsperren der Passwort Datenbank

Wenn das Passwort eingegeben ist, wird die Datenbank von KeePass geladen. Auf der linken Seite sieht man die (vorgegebenen) Namen der Passwort Gruppen. Auf der rechten Seite werden die Passwörter in der aktuell gewählten Gruppe aufgelistet. Dazu gehört ein

- frei wählbarer Bezeichner,
- der Nutzername,
- das Passwort,
- die URL der Seite auf der das Passwort verwendet wird und
- eine Notiz zum Passwort.

Über die Maus kommt man in ein paar Klicks zu den Dialogen zum Ändern der Einträge, dem anlegen neuer Einträge usw..

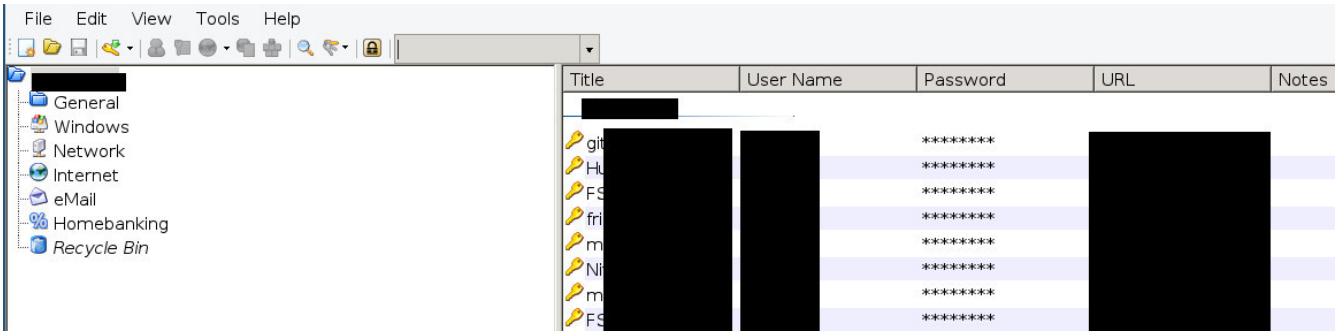


Abbildung 8. Auszug aus meiner Passwort Datenbank

Im Vortrag kommt jetzt ein bisschen Vorführeffekt um KeePass zu zeigen.

Mehr als ein Endgerät

Nun besitzen viele von uns mehr als ein Endgerät auf dem die Passwörter sinnvoller Weise

verfügbar sein sollten. Die Datenbanken müssen also zwischen den Geräten synchronisiert werden. Die Art und Weise der Synchronisierung hängt dabei stark von der Art der Endgeräte ab.

Wenn man eine *Master-Passwort-Datei* hat kann man das relativ einfach machen, indem man die Datei auf einem beliebigen Weg austauscht. Insbesbesondere, wenn diese Datei nur auf einem Gerät editiert wird. Das kann automatisch vom PC in die eigene Cloud geladen werden und von den Zweitgeräten regelmäßig runter geladen werden bedeuten. Oder man trägt die Datenbank mit den Passwörtern auf dem USB Stick von A nach B.

Oder man hat einfach nur die eine Passwortdatenbank auf dem USB Stick. Es muss ja nur der Passwort Manager auf allen Endgeräten installiert sei, der auf diese Datenbank zu greifen kann wenn der USB Stick eingesteckt ist. (*Backup nicht vergessen* der USB Stick kann ja mal verloren gehen…)

Viele Passwort Manager bieten auch die Funktion des Synchronisierens direkt an. Kann über die Cloud sein, oder lokal zwei Dateien synchronisieren. Dabei verwenden sie dann wahrscheinlich den *zuletzt geändert* Eintrag für die einzelnen Passwörter in den beteiligten Datenbanken um zu entscheiden, welcher Eintrag der aktuell gültige ist.

Passwort Manager sind…

Wo wir jetzt alle Passwörter im Passwort Manager gespeichert haben.

Denkt an die Backups der Passwort Datenbank. So ein USB Stick mit der einzigen Passwort Datenbank kann kaputt gehen, oder ihr lasst ihn im Restaurant liegen. Und eventuell sollte das Backup auch dann funktionieren, wenn der Passwort Manager nicht funktioniert.

Dann solltet ihr nicht vergessen, dass so eine Datenbank voll mit Passwörtern ein lohnendes Ziel für die bösen Buben ist. Immerhin sind da ja jetzt all eure Passwörter drin enthalten. Also jeder der das Masterpasswort hat, der kennt all eure Passwörter, die dazugehörigen Nutzernamen und die URLs der Dienste wo ihr die Kombination verwendet habt.

Links

- Identity Leak Checker des Hasso Plattner Instituts, Universität Potsdam
- Surveillance Self-Defense (Electronic Frontiers Foundation)
- Creating Strong Passwords (EFF)
- Wechselwahn (iX, 4/2017)
- Kleines 1x1 der digitalen Selbstverteidigung (netzpolitik.org)
- Wikipedia (EN) List of Password Managers
- Wikipedia (EN) Liste der meist genutzten Passwörter
- haveibeenpwned.com
- Empörung nach der Cyberattacke (tagesschau.de, 4.1.2019)
- Hackerangriff auf Hunderte Politiker (tagesschau.de am 4.1.2019)

- Tatverdächtiger nennt Verärgerung über Politiker als Motiv (rbb24 am 8.1.2019)
- Die vier Freiheiten der Freien Software (FSFE)
- I love Free Software Day FSFE Kampagne
- XKCD Comics by Randall Munroe