Ein gutes Passwort

- schöpft die volle Möglichkeit von acht (besser 10) Zeichen aus
- enthält mindestens zwei Buchstaben unter Verwendung von Groß- als auch Kleinbuchstaben
- enthält mindestens zwei Ziffern oder Sonderzeichen, diese stehen nach Möglichkeit nicht nur am Anfang und/oder Ende
- kann man sich leicht merken
- kann man schnell eintippen (das Passwort ist durch Über-die-Schulter-schauen nicht leicht erkennbar)
- enthält keine (erkennbare) Systematik, d.h. erscheint wie eine zufällig erzeugte Zeichenfolge
- ist kein Wort einer bekannten Sprache
- ist nur dem Inhaber der Kennung bekannt
- wird in angemessenen Abständen geändert. Was angemessen bedeutet, richtet sich nach den Sicherheitsanforderungen. Für eine normale Benutzerkennung reicht eine Änderung ca. alle sechs Monate.

Allgemein: für verschiedene Kennungen sollte man verschiedene Passwörter wählen.

Im Anschluss stellen wir Ihnen einige Verfahren zur Erzeugung von sicheren Passwörtern vor, die den oben genannten Anforderungen genügen und trotzdem leicht zu merken sind:

Grundsatz: Nicht das Paßwort wird gemerkt, sondern die Methode, mit der es gebildet wird!

Akronym-Methode

Man bildet einen Satz und verwendet als Passwort die Anfangs- oder auch Endbuchstaben der einzelnen Wörter, zusätzlich fügt man noch mindestens zwei Ziffern oder Sonderzeichen ein.

Beispiele:

- MbeS&&va = Akronym für den Anfang des vorhergehenden Satzes
- v9b10:Rv = von 9 bis 10: Rauchen verboten
- W?nA-zA! = Wohin? nach Aldi nein zu Aldi!

Es kann auch eine Zeile aus einem Gedicht, einem Lied oder ein (jedoch bitte nicht allzu gebräuchlicher) Spruch gewählt und darauf die Akronym-Methode angewendet werden. Sicherheitshalber sollte man immer noch Sonderzeichen oder Variationen einstreuen.

Methode Doppelwort

Suchen Sie sich zwei Wörter (Autoren, Schauspieler, Hobbys, ...) aus, die geschickt gekürzt, verschachtelt und zusätzlich mit Sonderzeichen versehen werden.

Beispiel:

- Ba+Fo;Zc (Bildungsregel: aus Balzac und Fontane)
- S:LaO!Ha (Bildungsregel:Stan : Laurel Oliver ! Hardy)

Collage-Methode

Man wählt ein Wort aus einer natürlichen Sprache und übersetzt dieses Wort in eine, besser noch in zwei andere Sprachen. Anschließend entnimmt man diesen Wörtern zwei oder drei Buchstaben (Wortanfang, Wortmitte, Wortende) und verbindet sie mit Ziffern oder Sonderzeichen. Zur weiteren Erhöhung der Sicherheit kann man noch gleichzeitig Groß- und Kleinbuchstaben verwenden.

Beispiel:

- hou:17Hau (Bildungsregel: house bzw. Haus; Ihre Hausnummer ist 17)
- P:rs$val (Bildungsregel: Pferd : Horse $ cheval

Besitzen Sie mehrere Kennungen und sind dadurch gezwungen, sich viele verschiedene Passwörter zu merken, empfiehlt es sich, systematisch Passwort-Familien zu erzeugen. Sie bilden nach den oben erläuterten Methoden ein 6-7 Zeichen langes Passwort. Dieses kann dann durch 1-2 Zeichen ergänzt werden, die Ihnen die Unterscheidung der verschiedenen Kennungen ermöglichen (Rechnernamen oder Zweck der geschützten Anwendung).

Umstritten: Die Methode Zufall

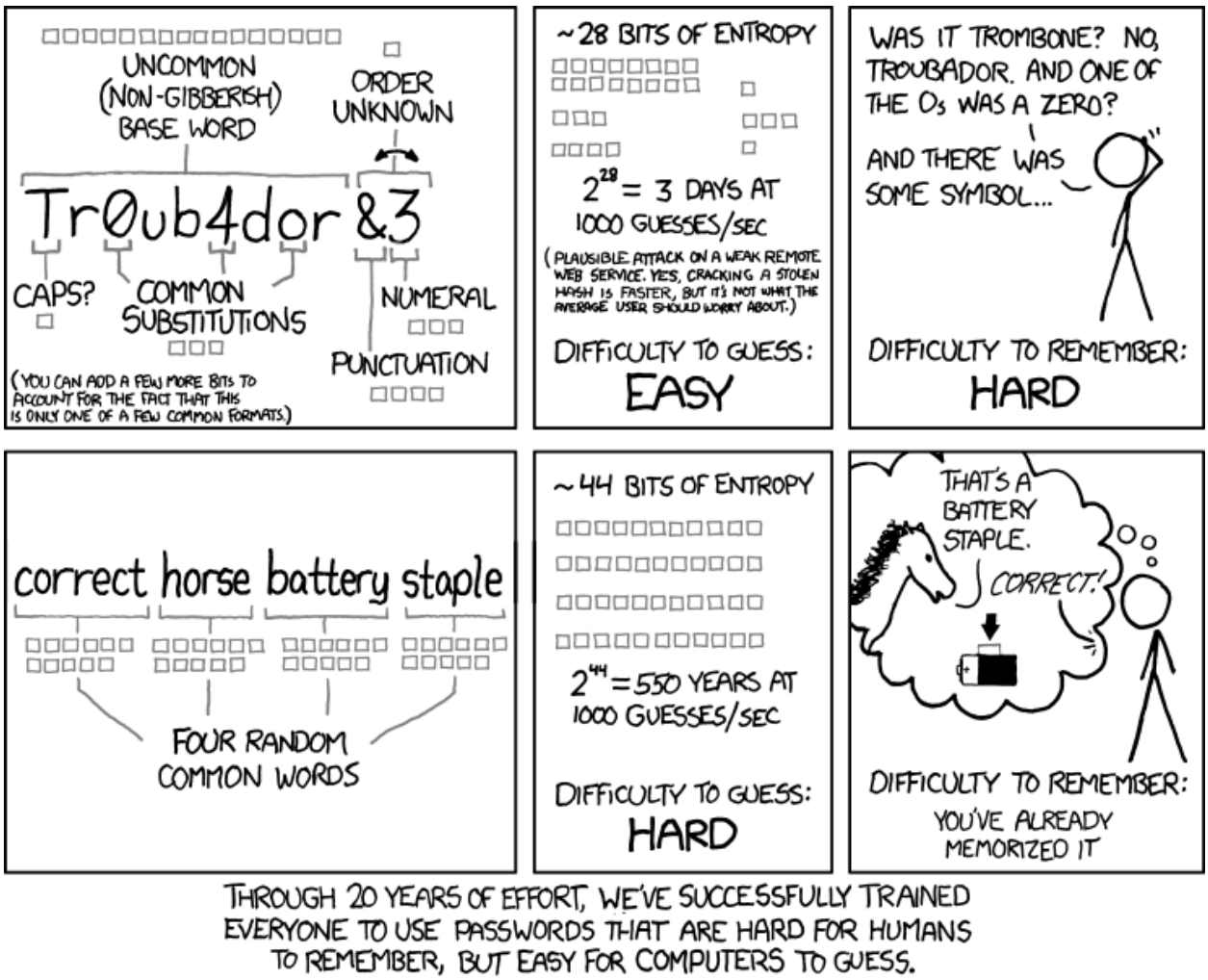
Wenn Sie acht Zeichen per Zufall oder zumindest sehr willkürlich auswählen, dann erhalten Sie ein in der Sicherheit nicht mehr zu überbietendes Passwort. Vermeintlich. Denn angesichts der Tatsache, dass solche Passwörter sowohl beim Auswendiglernen als auch bei der Blindeingabe oftmals große Schwierigkeiten bereiten, sind sie nur scheinbar sicher. Muss man in Anwesenheit anderer Personen ein Passwort eingeben und ist dann auf das "Adler-Such-System" bei der Eingabe angewiesen, erleichtert dieses den Anwesenden das unauffällige Mitlesen der eingegebenen Zeichenfolge. Oder - worst case - man kann sich das supersichere Passwort gar nicht merken und notiert es sich irgendwo.

Ein Tipp, für den Fall, dass Sie dieser Methode den Vorzug geben: Nur durch häufige Benutzung lassen sich komplizierte Passwörter zuverlässig merken. Sie sollten sich nach einer Passwortänderung ruhig ein halbes Dutzend mal einloggen und es später mindestens wöchentlich tun, um das Passwort zuverlässig im Gedächtnis zu behalten.

XKCD Methode

XKCD ist eine im akademischen Umfeld bekannte Webcomic-Serie ("A webcomic of romance, sarcasm, math, and language.").

In Comic Nr. 936 Password Strength (Passwortstärke) [1] wird der aktuelle Stand in der IT-Sicherheit beschrieben nachdem (vereinfacht) für Menschen "schlecht" merkbare (kryptische) Passwörter von Computern (automatisiert) leicht geknackt werden können und von Menschen leicht merkbare (aber lange) Passwörter von Computern schwer geknackt werden können.



Lizenz CC BY-NC 2.5 [2] / XKCD 936: Password Strength [1]: "To anyone who understands information theory and security and is in an infuriating argument with someone who does not (possibly involving mixed case), I sincerely apologize."

Die aktuelle Empfehlung sollte also lauten: Denken Sie **nicht** an Passwörter, sondern an Passphrasen.

Ganz im Zeichen von "Sesam-öffne-dich!" empfehlen wir:

- Nehmen Sie sich 5 bis 6 Worte, die Sie sich gut merken können, und verbinden sie diese mit Bindestrichen zu einem Wort.
- Sie können natürlich auch Zahlen und Satzzeichen mit einfließen lassen.

Beispiele:

Satz	Passphrase / Passwort
Netzwerke werden heute mit ROADMs gebaut ! 42	**NETZWERKE-werden-HEUTE-mit-ROADMS-gebaut!42**
Warnung Regen Planet Pflanze Matetee 128	**warnung-REGEN-PLANET-pflanze-MATETEE-128**

XKCD Passwortgenerator:

Unter xkpasswd.net [3] finden Sie einen Passwortgenerator. Hier einfach das **Preset: XKCD** wählen.

Die verwendete xkpasswd-Perl-Bibliothek [4] findet sich im CPAN unter Crypt::HSXKPasswd [5] und natürlich auf GitHub unter bbusschots/hsxkpasswd [6]

Wenn Sie einer Website, die Passwörter erstellt, nicht trauen und nicht kreativ genug sind, aus den Texten/Büchern/Zeitungen/... um Sie herum zufällig Wörter für eine Passphrase herauszupicken, können Sie nach der Installation des Perl-Moduls in der Kommandozeile Ihres Vertrauens mit folgendem Befehl Passwörter selbst zufällig erstellen:

```
hsxkpasswd -p xkcd -o '{"padding_digits_after": 2}'
```

Grundsatzproblem: Passwortschlüsselbund und mehrfache Verwendung von Passwörtern

In der heutigen Welt melden wir uns bei verschiedensten Dienste/Webseite/... an. Oft wird dasselbe Passwort für verschiedene Dienste (E-Mail-Konten, Online-Banking, Online-Händler, soziale Netzwerke, Moodle/E-Learning, ...) verwendet.

Webseiten wie haveibeenpwned.com zeigen anschaulich, wie viele Passwörter schon in den Händen von Verbrechern sind. Diese haben es bei einer mehrfachen Verwendung von Passwörtern natürlich einfach, weil sie für eine E-Mail-Adresse (die oft der Benutzername/Anmeldename ist) nur automatisiert bei verschiedenen Webseiten ausprobieren, wo das Passwort noch funktioniert.

Die einzige Möglichkeit, dies zu umgehen, ist, für jeden Dienst / jede Webseite ein anderes Passwort zu verwenden.

Da man sich als Mensch aber nur endlich viele "gute" Passwörter merken kann, gibt es sogenannte Passwort-Manager oder Passwort-Schlüsselbünde. Hierbei handelt es sich um Software.

Üblicherweise muss man sich bei Benutzung eines Schlüsselbunds nur noch ein (möglichst gutes) "Master-Passwort" merken, mit dem alle anderen Passwörter gesichert sind und mit dem man den Schlüsselbund entsperren kann.

Arten von Passwort-Managern / Passwort-Schlüsselbünden

offline

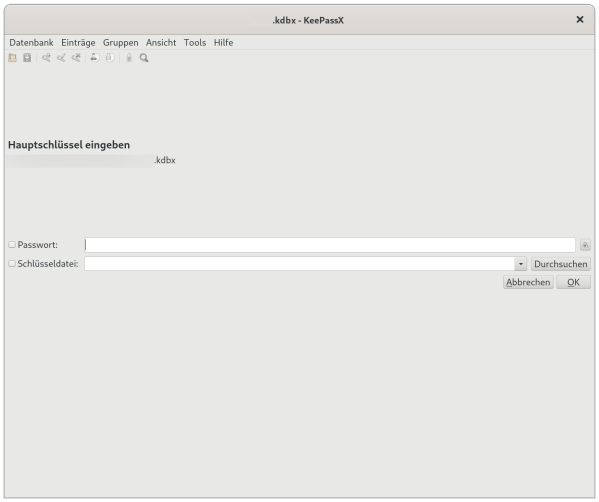
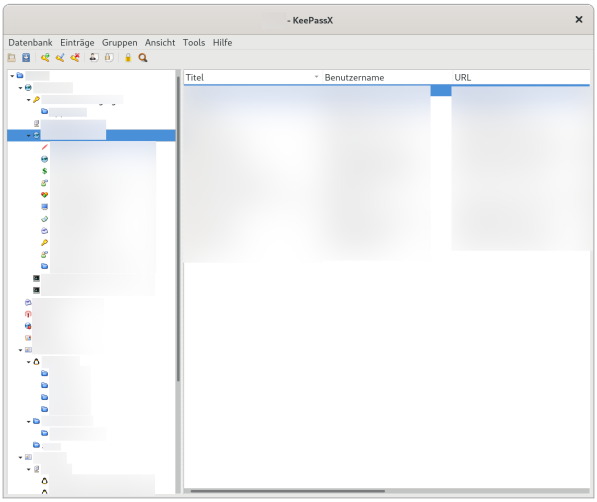
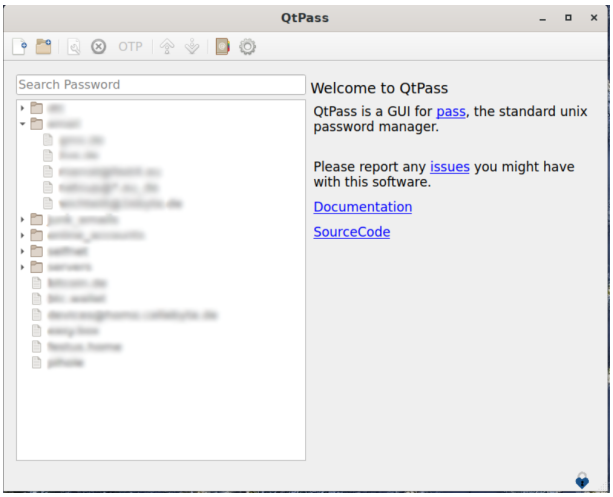
In diesem Fall liegt die Kontrolle über die verschlüsselten Dateien komplett bei Ihnen!

Die verschlüsselten Dateien können dann auch auf einem USB Stick, eigenem Cloud Speicher (z. B. Nextcloud) mitgenommen/synchronisiert werden, da die Verschlüsselung und Entschlüsselung lokal auf dem Computer stattfindet.

Beispiele:

Software Name	Oberfläche	Dateien / Verschlüsselung
KeePassX keepassx.org [7]	grafisch	.kdbx Dateien / AES [8]
KeePass keepass.info / KeePassXC keepassxc.org	grafisch	.kdbx Dateien / AES [8]
Apple Keychain / Schlüsselbundverwaltung	grafisch	AES [8]
pass www.passwordstore.org	Kommandozeile	nutzt PGP [9] zur Verschlüsselung
QtPass qtpass.org	grafische Oberfläche	nutzt pass/PGP [9] im Hintergrund

Hinweis: Für KeePassX, KeePassXC und KeePass (.kdbx Dateien) gibt es für Browser wie Firefox [10] und Chrome/Chromium [11] entsprechende Erweiterungen.

Screenshots:	KeePassX
	
	Apple Macintosh Schlüsselbund / Keychain
	QtPass
	

In der "Cloud"

Vereinfachte Definition Cloud: *Ein Computer, über den Sie selbst keine volle Kontrolle haben, der jemand anderem gehört, der Ihnen Rechenzeit und Speicherplatz vermietet.*

Es gibt diverse Anbieter, die für Geld einen online verfügbaren Schlüsselbund zur Verfügung stellen. Wie vertrauenswürdig die einzelnen Anbieter sind, können wir nicht beurteilen.

Der große Vorteil besteht darin, dass es sehr komfortabel ist, da der Schlüsselbund meist automatisch auf allen Geräten (Smartphone, Desktop, Laptop, ...) des Nutzers synchronisiert wird (nach Installation der notwendigen Anwendung/App/Erweiterung).

Meistens wird auch angegeben, dass die Verschlüsselung lokal auf den jeweiligen Geräten und nicht in der Cloud stattfindet. Inwieweit ein Laie dies nachprüfen kann, ist aber fraglich.

Es empfiehlt sich hier auf jeden Fall, über die "Marketing-Aussagen" eines Unternehmens hinaus zu recherchieren.

Im besten Fall liegt die verschlüsselte Passwortdatei (siehe "offline") in einer eigens verwalteten "Cloud" (z. B. Nextcloud) oder bei einem Cloudanbieter, dem man persönlich vertraut.

Zusammenfassung

Die Nutzung von jeder Art von Passwort-Schlüsselbund (Offline oder in der Cloud) ist besser, als diese nicht zu nutzen.

Allgemeiner Hinweis

Diese Bildungsregeln sollen Ihnen nur als Anregung dienen. Es ist sehr erwünscht, dass sich jeder Benutzer Gedanken über einen eigenen Algorithmus macht oder die Vorschläge zumindest abwandelt. Dadurch wird verhindert, dass neue Generationen von Knack-Programmen, die auch auf diese schon häufig empfohlenen Bildungsregeln eingehen, erfolgreich sind. Insbesondere verwenden Sie nicht die Passwörter, die in diesem Beitrag als Beispiele aufgeführt wurden ;-).

- Autor: Dipl.-Inf. Christine Peter, Leibniz Universität Hannover, IT Services [12]
- Erweitert durch: BelWü-Koordination

Links

[1] https://xkcd.com/936/
[2] https://creativecommons.org/licenses/by-nc/2.5/
[3] https://www.xkpasswd.net/
[4] https://www.bartbusschots.ie/s/publications/software/xkpasswd/
[5] https://metacpan.org/pod/Crypt::HSXKPasswd
[6] https://github.com/bbusschots/hsxkpasswd
[7] https://www.keepassx.org/
[8] https://de.wikipedia.org/wiki/Advanced_Encryption_Standard
[9] https://de.wikipedia.org/wiki/Pretty_Good_Privacy
[10] https://addons.mozilla.org/de/firefox/addon/keepassxc-browser/
[11] https://chromewebstore.google.com/detail/chromekeepass/dphoaaiomekdhacmfoblfblmncpnbahm
[12] https://www.luis.uni-hannover.de/de/ueber-uns/team/personen-detailansicht/abteilung-arbeitsplatzrechner-und-sicherheit-21pk3/04c7d504-b18a-69ad-73f0-b00d949744ba/dipl-inf-christine-peter?tx_t3luhepv_t3luhepvoe%5BdisablePersHomepages%5D=0&cHash=5b19b8fedd9c31af7ce15ef132ead0b5

Quelle: https://support.belwue.de/anleitungen/gutepasswoerter/