Wie sicher ist mein Passwort?

Marc Nilius - @marcnilius - @WPSicherheit
Barcamp Bonn 2016

Wie sicher ist dein Passwort?

Wieviele Zeichen?

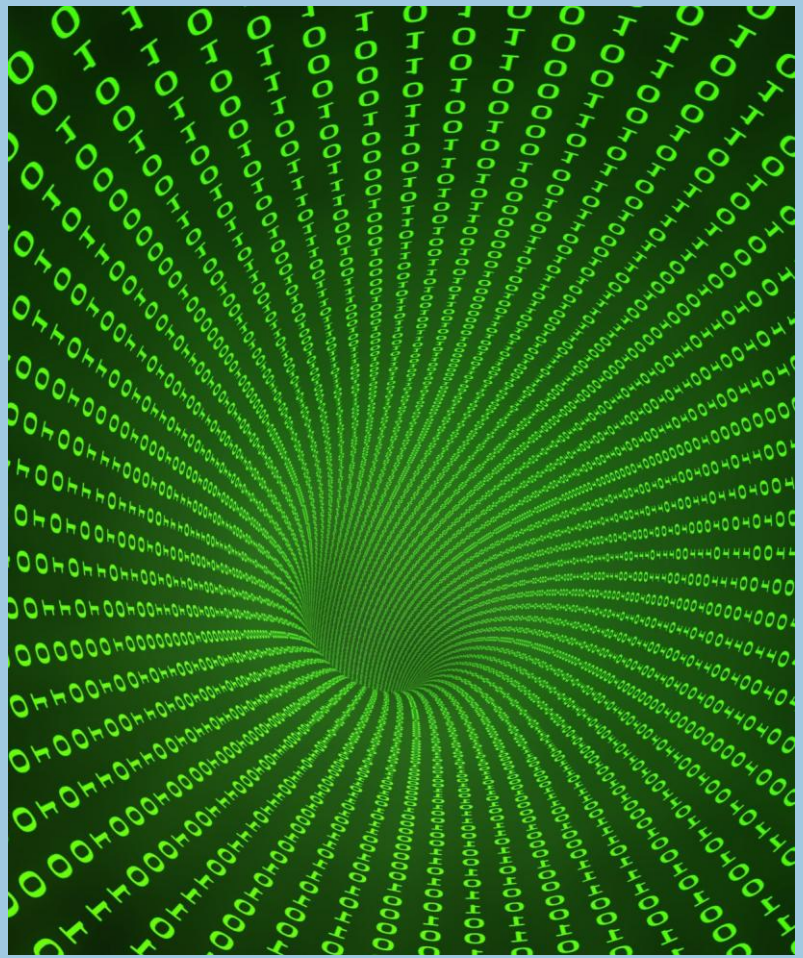
Welche Zeichen?
Kleinbuchstaben? Großbuchstaben?
Sonderzeichen?

Was ist ein Brute-Force-Angriff?

Brute-Force-Angriff:
Zugriff durch Ausprobieren aller Möglichkeiten mit „roher Gewalt“

Online:
z.B. WordPress-Login, Zugriff über das Internet (langsam)

Offline:
Durch vorangegangenen Hack/Diebstahl Zugriff auf die Datenbank.
Dann Durchprobieren der Passwörter auf lokalem Computer (schnell)



Wie lange dauert es, bis ein Passwort geknackt ist?

Passwort, 8 Zeichen lang, bestehend aus:
Großbuchstaben A-Z, Kleinbuchstaben a-z, Zahlen 0-9
`HDMuMp9Y`

Online (1000 Versuche/Sekunde): 7000 Jahre
Offline (großes Array): 2,22 Sekunden

Mit Sonderzeichen:
`rJl=32aY`

Online (1000 Versuche/Sekunde): 213.000 Jahre
Offline (großes Array): 1,12 Minuten

Wie lange dauert es, bis ein Passwort geknackt ist?

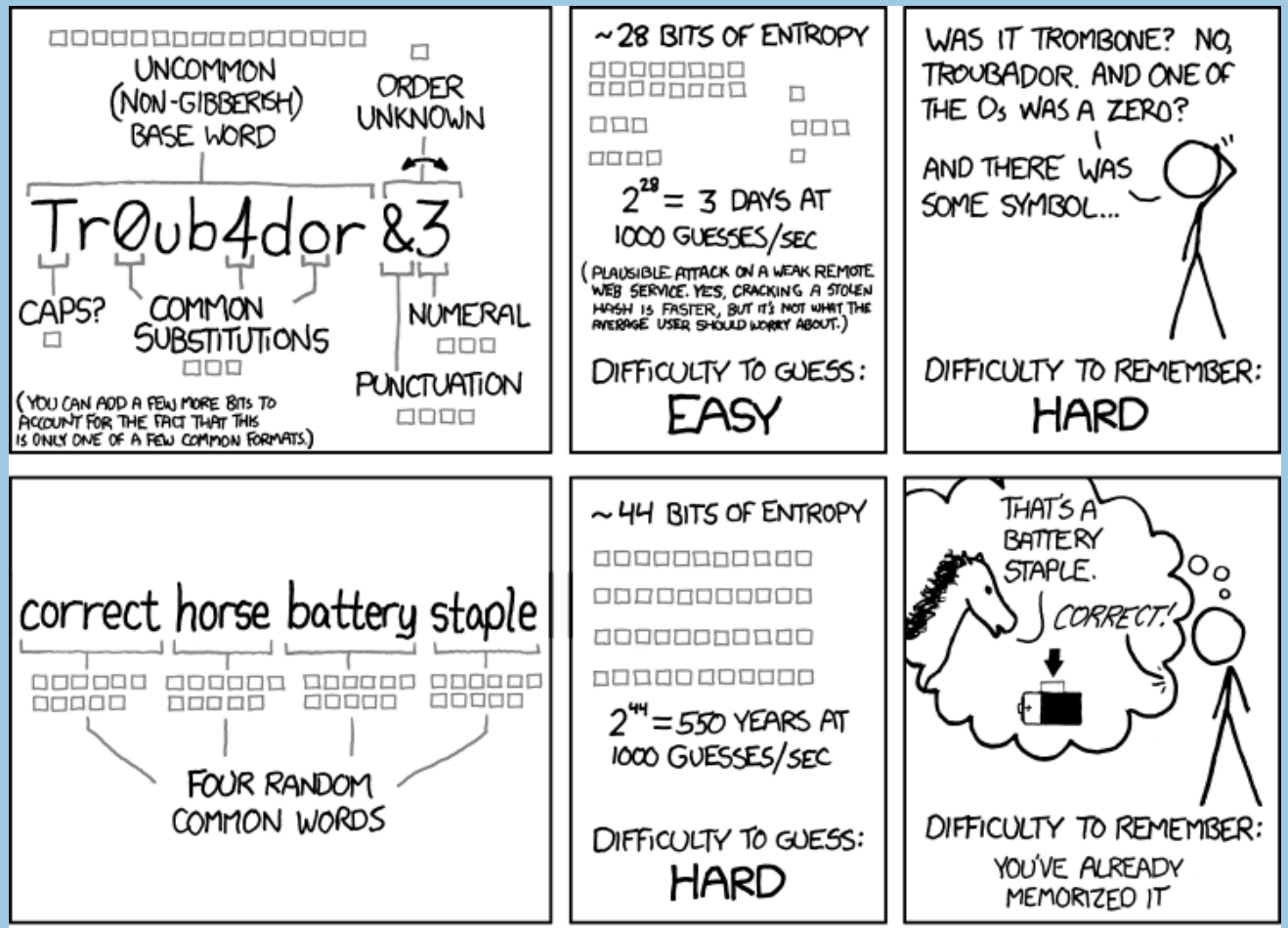
Demo: https://www.grc.com/haystack.htm

Wie lange dauert es, bis ein Passwort geknackt ist?

Wie sieht ein sicheres Passwort aus?

RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗
15	1qaz2wsx	NEW
16	dragon	7 ↘
17	master	2 ↗
18	monkey	6 ↘
19	letmein	6 ↘
20	login	NEW
21	princess	NEW
22	qwertyuiop	NEW
23	solo	NEW
24	password	NEW
25	starwars	NEW

Wie sieht ein sicheres Passwort aus?



Wie sieht ein sicheres Passwort aus?

- mindestens 12 Zeichen lang
- je länger, desto besser
- keine Einzelwörter (wegen Wörterbuchattacken)
- aber Passphrasen / ganze Sätze
    - keine Zitate
    - keine anderen Sätze, die sich in Büchern finden
- Am besten mehrere Wörter ohne direkten Zusammenhang
- wer ein klassisches Passwort verwenden möchte:
    - Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen

Wie bleibt mein Passwort sicher?

- Passwort nicht wiederverwenden
- Passwort alle 6 – 12 Monate bei allen Services ändern

Beispiel:
Basis-Passwort: 5aXGdeJYZwrG
Für Ebay: ebay_5aXGdeJYZwrG nächstes PW: ebay_5aXGdeJYZwrG-02
Für Facebook: fb_5aXGdeJYZwrG nächstes PW: fb_5aXGdeJYZwrG-02
Für Google: goo_5aXGdeJYZwrG nächstes PW_ goo_5aXGdeJYZwrG-02
Usw.

Weitere Möglichkeit: Single-Sign-On mit Facebook, Google, Twitter o.ä.
Nachteile: evil ;-)

Passwort-Manager - wie verwalte ich Passwörter?

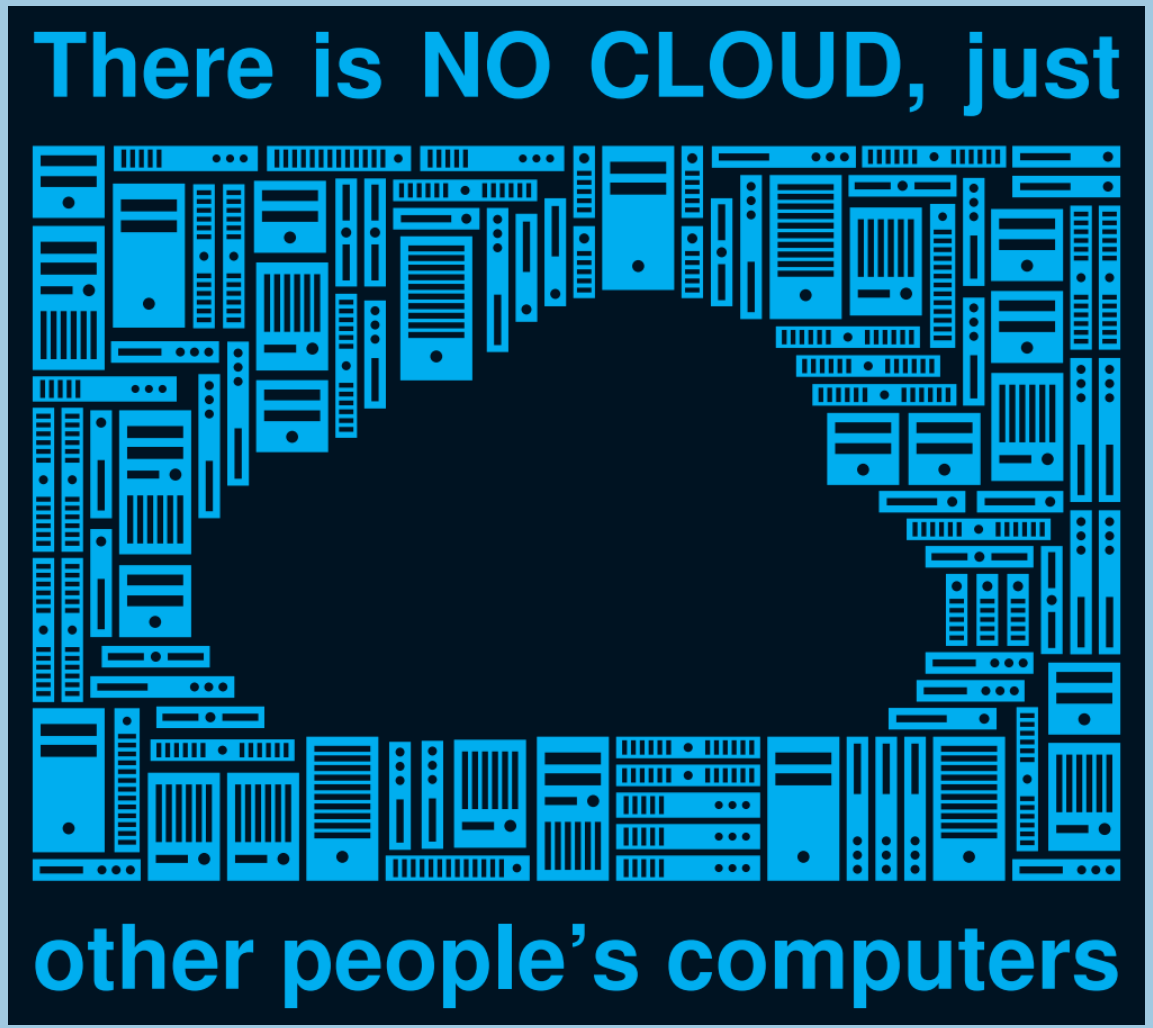
Mit Passwort-Managern kann man komfortabel alle notwendigen Passwörter verwalten und auch sichern

Besser als das „Blatt Papier“ neben dem Rechner

Nachteil: Wird der Rechner kompromittiert, sind alle Passwörter auf einmal unsicher

Deswegen: Der Passwort-Manager muss besonders gut gesichert werden (sehr langes Passwort, 2-Faktor-Authentifizierung mit Smartphone, Key-Datei auf USB-Stick)

Passwort-Manager - wie verwalte ich Passwörter?

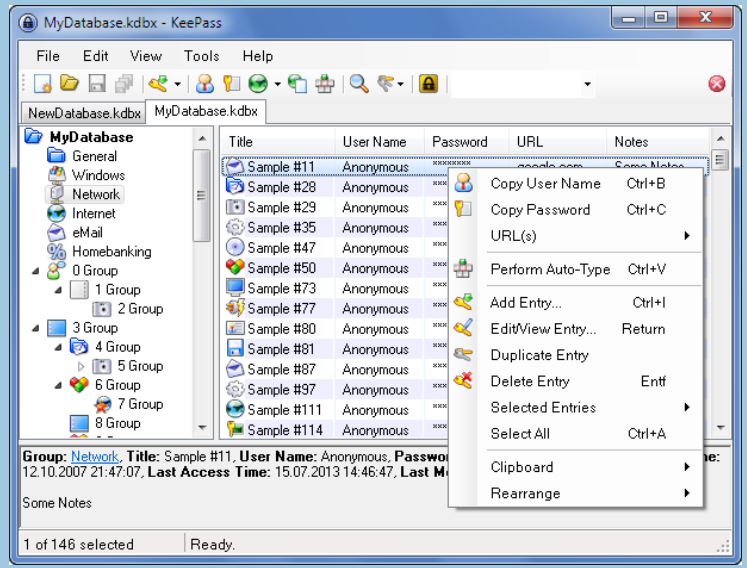


Passwort-Manager - wie verwalte ich Passwörter?

Darauf sollte man bei der Auswahl achten:

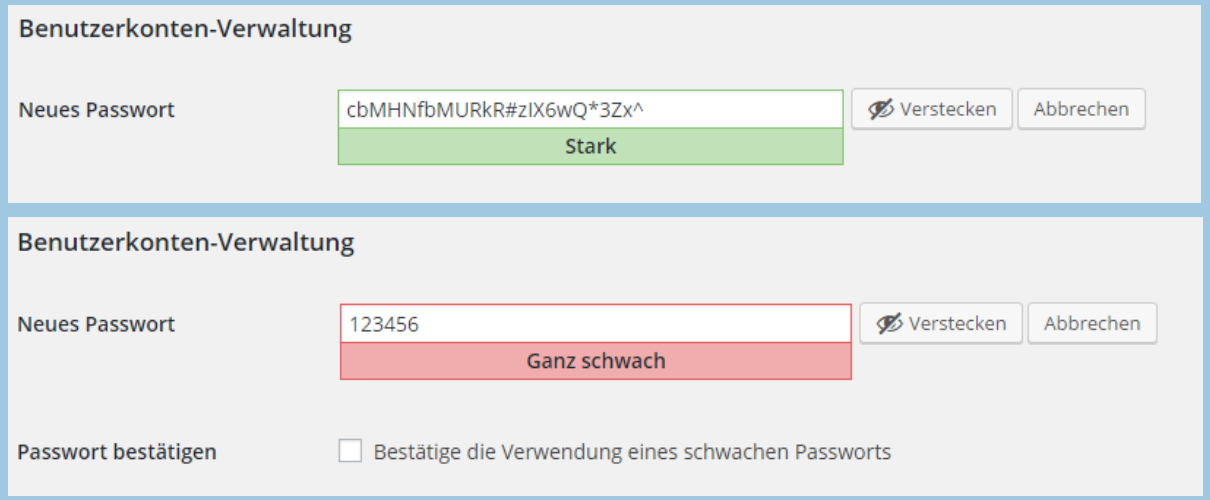
- keine Cloud-Lösung (auch wenn es praktisch erscheint)
- Gute Verschlüsselung (AES256 oder besser)
- Verschlüsselung nicht nur der Passwörter, sondern auch der Metadaten!
- Zugriff auf mit Passwort, besser aber 2-Faktor-Authentifizierung
- Open-Source bietet die Sicherheit, dass der Code intensiv geprüft wurde

Ich nutze: KeePass
(http://www.keepass.info)



WordPress: Wie stehts um die Passwörter?

- WordPress generiert selbst starke Passwörter beim Anlegen eines Benutzers
- Unsichere Passwörter sind durch den Benutzer möglich (aber nicht sinnvoll!)



WordPress: Wie stehts um die Passwörter?

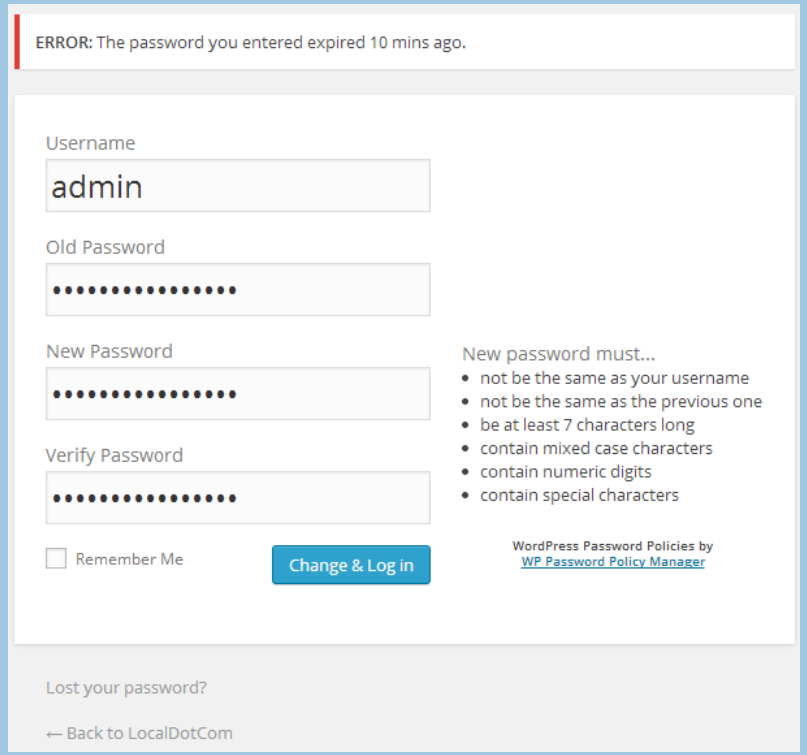
Sicherheits-Suiten (Wordfence, iThemes Securit, …) haben eine Einstellung, um starke Passwörter zu erzwingen

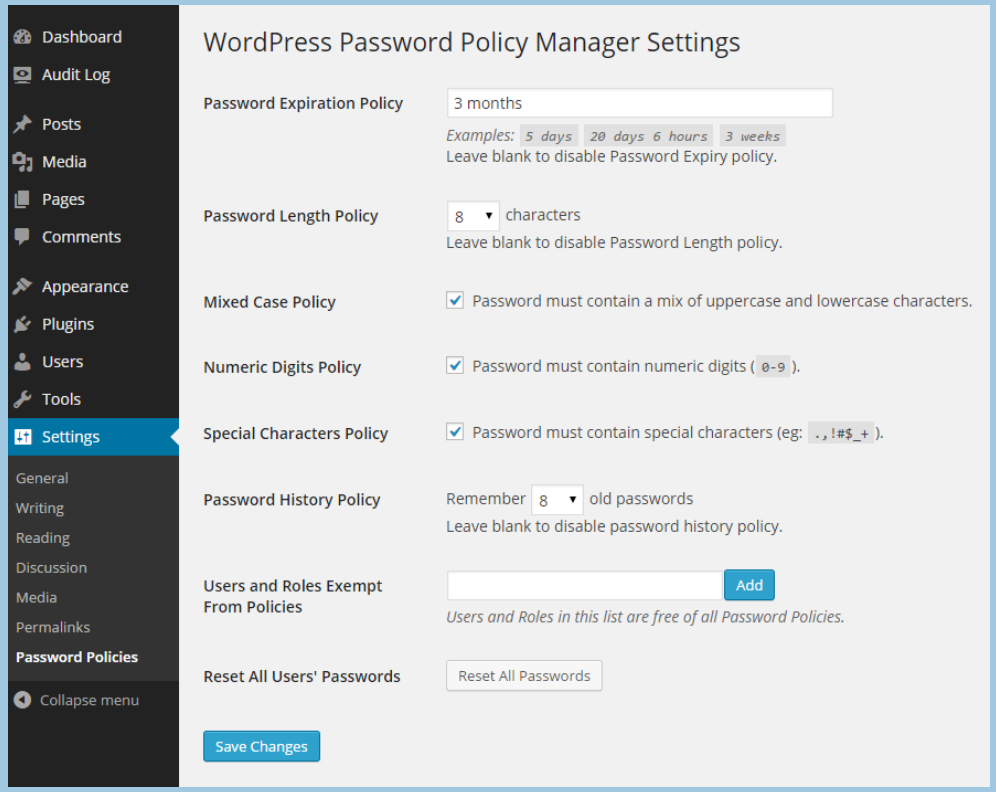
Meine Empfehlung: Das Plugin WP Password Policy Manager (https://de.wordpress.org/plugins/wp-password-policy-manager/)

Diverse Möglichkeiten für starke Passwörter:
- Mindestlänge, bestimmte Zeichentypen müssen enthalten sein
- regelmäßig neue Passwörter (werden beim Login eingegeben)
- neues Passwort muss anders sein, als die letzten X Passwörter

WordPress: Wie stehts um die Passwörter?

WP Password Policy





Mehr zum Thema WordPress-Sicherheit

Kostenloser Newsletter rund um WordPress-Sicherheit alle zwei Wochen:
https://www.wp-sicherheit.info

Twitter: @WPSicherheit und @marcnilius
Facebook-Gruppe: "WordPress Sicherheit"