How-To Passwort



Unsichere und sicherere Passwörter

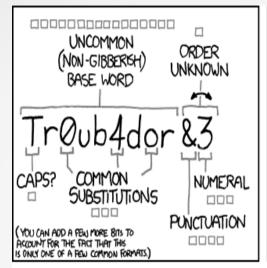
Die Länge ist entscheidend



- Ein gutes Passwort sollte aus min. 12 Zeichen bestehen
- Es sollte aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt sein.
- Es sollte nicht erratbar sein und keinen persönlichen Bezug haben.
- Sicher ist nichts, alles kann mit genug Geld und Zeit geknackt werden.
- Ein Passwort soll grundsätzlich nur einmal verwendet werden!

Ein Comic – xkcd #936



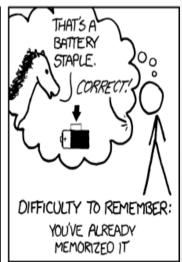


~ 28 BITS OF ENTROPY 28 BITS OF ENTROPY 29 = 3 DAYS AT 1000 GUESSES/SEC (PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE, YES, CRACKING A STOLEN HAGEN IS FASTER, BUT IS NOT WHAT THE	WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO? AND THERE WAS SOME SYMBOL
HOSH IS FASTER, BUT ITS NOT WHAT THE AVERAGE USER SHOULD WORKY ABOUT.) DIFFICULTY TO GUESS:	DIFFICULTY TO REMEMBER:
EASY	HARD

	correct horse battery staple
FOUR RANDOM	
	COMMON WORDS

00000000000
0000000000
00000000000
2 ⁴⁴ =550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
OPT VIEWE SIXCESSEUL

~44 BITS OF ENTROPY



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Die Passwortformel



- Denkt man sich selbst aus. Sei kreativ!
- Verrät sie nicht.
- Beispiel:
 - Sich einen festen Bestandteil ausdenken
 - z.B. H4nkDerD0ckarb3iter
 - Besser => H4nDerD0carb
 - Ein "Trennzeichen"
 - z.B. *
 - Ein veränderlichen Teil der sich auf den Zugang bezieht.
 - z.B. Ge_sichts_buch
- Ergibt ein "sicheres" Passwort mit 27 Zeichen:
 - H4nDerD0carb*Ge_sichts_buch

Sollte man das grundsätzlich tun?



- Jain, man sollte Grundsätzlich ein Passwort wählen was nicht zu einfach zu erraten ist.
- Man muss zwischen wichtig und unwichtig entscheiden
 - Wichtig:
 - Bank
 - Socialmedia
 - Überall da wo es um persönliche Daten geht
 - Unwichtig:
 - Wellensittichforum
 - Newsletter
 - Etc.

Für unwichtiges eine zweite Former Nordeingang Neuss e.V.

- Darf auch etwas "einfacher" sein.
 - z.B. FaselBla*Wellensittich
- Manchmal ist auch qwertz1234 O.K. wenn es total unwichtig ist.
 - z.B. für einen Newsletter o.Ä.
- Man will vermeiden das die wichtigen Zugänge kompromittiert werden.

Ich kann mir aber nichts merken! (**) Nordeingang



- Das ist erst mal schlecht.
- Technik kann helfen.
 - Passwortmanager
 - KeyPassX (Grafisch)
 - Pass (Kommandozeile)
 - 1Password (Mac/iOS)
- Browser bieten auch Passwortmanager, sind aber nur bedingt vertrauenswürdig.
 - Masterpasswort muss gesetzt sein.
 - Mozilla Sync für Synchronisation zwischen Smartphone und Laptop/Rechner
 - Kann man auch auf eigenem Server betreiben um ganz sicher zu gehen.

Links



- Bruce Schneier https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
- xkcd #936 http://xkcd.com/936/
- Slide Download https://github.com/vileda/slides/howto_password

Danke!



Fragen?