

Datensicherheit im Internet & Spielen

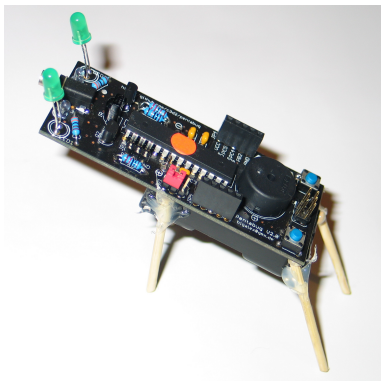
Wolf & Krihjin

28.06.2019

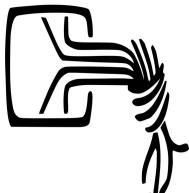
1. Crashkurs Thema Hacker
2. Der CCC - was ist das?
3. Aktuelle Nachrichten zum Thema
4. Passwörter
5. Facebook's Traum vom Datensammeln
6. On-/Offline-Spiele
7. Plattformen wie Steam u.Ä.
8. Browserbasierte Spiele
9. Mobilegames
10. Personenbezogene Daten
11. Spiele-Piraterie
12. Faustregeln

1. Crashkurs Thema Hacker





2. Der CCC - was ist das?



- CCC = Chaos Computer Club
- Verein wurde 1981 gegründet
- Aktuell mehr als 6000 Mitglieder
- <https://www.ccc.de/de/hackerethik>

C3D2

 Erfä in Dresden <http://c3d2.de>


pentacast Podcast


pentaradio Radio



Konferenz <http://datenspuren.de>

3. Aktuelle Nachrichten

- Innenminister wollen Daten von KI's wie Alexa, Siri und Ähnliche auswerten. Das betrifft nicht nur Handy's, oder kleine Geräte wie bei Alexa, sondern Fernseher, Kühlschränke und Sprachassistenten. Quelle:

<https://www.spiegel.de/netzwelt/netzpolitik/innenminister-wollen-offenbar-daten-von-alexa-siri-und-co-auswerten-a-1270870.html>

- Bundestagspräsident Wolfgang Schäuble und Manfred Weber (Spitzenkandidat der EVP) wollen eine Klarnamenpflicht.

Quelle:

<https://www.spiegel.de/netzwelt/netzpolitik/klarnamenpflicht-im-internet-warum-anonymitaet-im-netz-so-wichtig-ist-a-1268306.html>

- Bundesinnenminister Horst Seehofer will die Verschlüsselungen durch Anbieter wie Whatsapp u.Ä. auf richterliche Anordnung aufheben lassen.

Quelle: <https://www.spiegel.de/netzwelt/netzpolitik/horst-seehofer-will-messengerdienste-zum-entschluesseln-zwingen-a-1269121.html>

4. Passwörter



Home

Notify me

Domain search

Who's been pwned

Passwords

API

About

Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)





359
pwned websites

7,840,611,051
pwned accounts

92,984
pastes

113,417,711
paste accounts

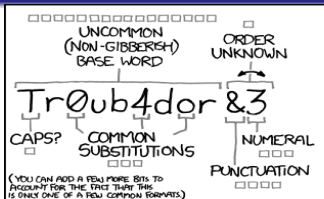
Largest breaches

-  772,904,991 Collection #1 accounts
-  763,117,241 Verifications.io accounts
-  711,477,622 Onliner Spambot accounts
-  593,427,119 Exploit.in accounts

Recently added breaches

-  760,561 DataCamp accounts
-  808,330 Knuddels accounts
-  52,623 Demon Forums accounts
-  871,190 Everybody Edits accounts

Sichere Passwörter



~ 28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

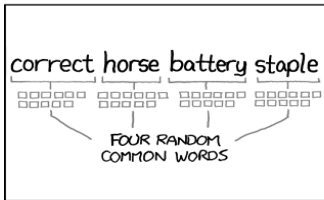
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~ 44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

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.

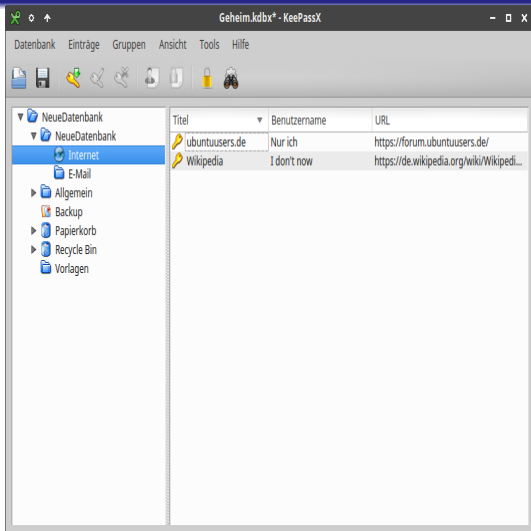
<http://xkcd.com>

Passwörter würfeln



- 43142 merken
- 15613 boom
- 12252 abluft
- 66445 zonen
- 51615 ragt
- 32644 hurra

Passwortmanager



Passwort-Generator

pwgen.jpg

Biometrie

biometrie.jpg

Biometrie

<https://media.ccc.de/v/biometrie-s8-iris-fun>

Zweifaktorauthentifizierung



Zweifaktorauthentifizierung



5. Facebook's Traum vom Datensammeln

- Facebook nutzt Apps, um noch mehr Daten zu sammeln

<https://www.spiegel.de/netzwelt/apps/facebook-bezahlt-nutzer-fuer->

- FB möchte eine neue Währung einführen : Libra.

<https://www.heise.de/newsticker/meldung/Projekt-Libra-Facebook-s>

Wer spielt welche Spiele?

6. On- und Offline-Spiele

- Über Modifikationen und Addons, kann vieles heruntergeladen werden - einschließlich Malware! Bilder zu den Addons oder Mods, sagen nichts darüber aus, was wirklich drin ist!
- Private Server bieten beliebte Spiele an, die i.d.R. mit monatlichen Kosten verbunden sind. Aber: Auch hier kann niemals sicher sein, ob bei der Installation / Patches durch den privaten Anbieter, nicht mehr installiert wird, als gewünscht.

- Malware kann auch über die Entwickler selbst eingeschleust werden, wenn die verwendeten Tools bereits Infiziert sind!
<https://www.spiegel.de/netzwelt/games/spieleentwickler-vertreiben-versehentlich-infizierte-spiele-a-1264181.html>

7. Plattformen wie Steam u.Ä.

- Auch über Plattformen wie Steam, kann Malware verbreitet werden. In bekannten Fällen über die Chatfunktion:

<https://www.pcgames.de/Steam-Software-69900/News/hacker-betrueger-account-malware-video-link-valve-1209954/>

8. Browserbasierte Spiele

Auch in Browserbasierten Spielen kann Malware verbreitet werden. Hier in der Regel durch Buttons: <http://www.was-ist-malware.de/it-sicherheit/sicherheit-online-games/>

9. Mobile Games

Handys sammeln wahnsinnig viele Infos über uns: Wo du häufig bist, wo du warst, deine Kontakte, deine Kalendereinträge u.v.m. Mit mehreren Standorten, lassen sich sogar Bewegungsmuster erkennen! Mobilegames können dabei ein Einfallstor für Schadsoftware sein:

<https://www.netzwelt.de/news/170032-malware-ueber-200-android-apps-habt-spiele-installiert.html>

10. Personenbezogene Daten

Es gibt Daten, die alle Arten von Spielen sammeln können, und das auch machen! - Standort. - Welches Gerät verwendet wird - mit welcher Konfiguration. - ...

11. Spiele-Piraterie

Mal davon abgesehen, dass es echt uncool ist, eine Dienstleistung in Anspruch zu nehmen, ohne dafür den angemessenen Preis zu zahlen, können Raubkopien von Spielen auch Malware einschleusen:

<https://www.kaspersky.de/blog/malware-in-pirated-games/18563/>

12. Zum Abschluss noch ein paar Faustregeln

- [1.] Anti-Viren-Programme (AVP) immer verwenden.
- [2.] Falls das AVP ausschlägt, immer das warum hinterfragen, nichts einfach blind zulassen.
- [3.] Backups sind niemals eine schlechte Idee. Selbst wenn alle deine Daten verschlüsselt wurden, kannst du den PC neu aufsetzen, und mit dem Backup alles wiederherstellen.
- [4.] Öffne keine Links in Emails, wenn du den Absender nicht zu 100 Prozent zuordnen kannst!

[5.] Makros sind ein beliebtes Einfallstool für Malware (siehe z.B. Emotet, Heise). Wenn du aufgefordert wirst, Makros zu aktivieren, lass lieber die Finger davon.