26. Mai 2021

digitale Selbstverteidigung: Passwörter

Clemens Schweigler
ak-digit@bv-schwarzwald.vdi.de

- Augen auf vor Passwortklau!
- Passphrasen zum Eigenschutz
- Zufall vor Einfalt
- Passwort-Management mit KeepassXC

Schwerpunkt meines Ehrenamts im VDI und FLUG
ist das Bewusstsein zu schaffen und Unterstützung zum
Thema Informationssicherheit und Datenschutz

Zuerst etwas Erwartungsmanagement:

Es gibt keine einfache Lösung für Alle...

Umfrage: Wo haben Sie von dieser Veranstaltung zuerst gehört?

Badische Zeitung → B
CCC / FLUG-Umfeld → C
VDI → D
Andere / Sonstige → A

Heute: Informations-Sicherheit durch Zugangskontrolle

Dies kann mit individuellen Benutzernamen und hinreichend komplexen Kennwörtern geschehen.

Bequemlichkeit geht meist auf Kosten der Sicherheit

Zielgruppe sind hier Privatleute an PC und Laptops.

Daher habe ich keine Crypto-Hardware (PGP, OTP, 2FA) im Programm...

Weitere FLUG-Treffen am 18.Juni, 23.Juni, 16.Juli – jeweils ohne Vortrag

Augen auf vor dem Passwortklau:

- Phishing-Mail/Anruf werden dank deepFake + KI immer schwerer erkennbar

- "unsichere" eigene HW/Software incl. Auslieferungs-PW

- Error 42: Leak beim surfen

- "Besuch" von Jederleut: Schadsoftware (Kriminelle, verdeckte Ermittler)

im Netz:

- Anbieter ist nachlässig mit IT-Sicherheit

- Anbieter schlampt im Umgang mit Passwörtern

- "Besuch" von Jederleut: Schadsoftware (Kriminelle, verdeckte Ermittler), National Security Letter

Deshalb digitale Selbstverteidigung: ein richtiges Passwort muss her!

"Best of" - Regeln + keine Diskussion!

- Das richtige Passwort gehört mir allein und ist einmalig für jeden Zugang
- Das richtige Passwort hat mindestens 12 Zeichen oder wird öfters gewechselt
- Die richtige Passphrase wähle ich zufällig und selbst
- Die richtige Passphrase gebe ich nur in bekannte Geräte ein,
  ohne dass Jederleut zusieht
- Die richtige Passphrase habe ich im Kopf und sicher verwahrt
- eins? Viele!

Deshalb: verwende ich eine Pass**dings**Datenbank

Das funktioniert wie ein Tresor:

Eine Datenbank für geschützte Zugänge wird per Master-Passphrase verschlüsselt.

Nur eine super richtige Passphrase muss zum Öffnen eingegeben und gemerkt werden.

Innen liegende Zugänge können dann aus der Datenbank heraus kopiert werden.

ja, die richtige Passphrase ist extrem wichtig

und die Datenbankdatei muss in einem Backup gesichert werden

Empfehlungen/Anleitungen für KeePassXC gibt es einige' im Netz, mir war wichtig:

- lokal gespeicherte Datenbank
- umfassende DB durchsuchbar
- FOSS: Freie Software, Quellcode liegt als Klartext vor
- Zugänge strukturiert „kuratiert“ ablegen
- XC nativ für viele Plattformen erhältlich

- automagisches Ausfüllen? testen, testen….
- aktive Kümmerer -> Spende an's XC-Team?

Vergleich KeePassXC: native Linux

vs. KeePassV2: - viele Addons – Silben-PW-Generator - Notfalldatenblatt

Umfrage: Wer nutzt Linux (ja) am PC /Notebook? Nein: kein Linux

Alles über Passwortstärke (Entropie)

- je größer der Zeichenvorrat, desto besser
- je länger, um so noch besser
--> Zeichenvorrat ^ Stellen = Kombinationen

- je zufälliger "gewürfelt", um so besser die Entropie

Wie?
Passwörter würfeln mithilfe einer Passwortliste
ergibt **Master-Passphrase** mit mind. 6 ausgewürfelten Wörterbucheinträgen

PW mit begrenzter Stellenzahl merken -> **Silben-Passwort**:
mehrere gewürfelte Silben mit Sonderzeichen und maximaler Stellenzahl (mind. 12) sieht so z.B. aus: Giki.wamu.fima.weke. (was ein Aufgäbchen f. Bash-Programmierer wäre...)

nicht mehr zu merken:
Alle anderen PW werden in der Keepass-DB generiert und gespeichert!

effektives **Merktraining** durch Wiederholung mit Belohnung:
kurzes Timeout der Bildschirmsperre mit neuer Passphrase!

Passwortstärke ergibt sich rechnerisch

Zeichenvorrat ^ Stellen = Kombinationen

	Zeichenvorrat	Silben	Stellen/Silbe	Stellen		Kombinationen	Entropie
Zahlen-PIN	10			4		10000	13
4 Dice-Wörter	7776			4		3,66E+15	52
Alphanum.	60			12		2,18E+21	71
An+Sonderz.	70			12		1,38E+22	74
6 Dice-Wörter	7776			6		2,21E+23	78
An+Sonderz.	70			16		3,32E+29	98
8 Dice-Wörter	7776			8		1,34E+31	103
4 Silben	70	4	5	20		7,98E+36	123
5 Silben	70	5	4	20		7,98E+36	123

maximale Entropie ist, wenn optimal zufällig gewürfelt wurde!

Welches PW nehme ich wann?

eine Master-Passphrase:
Keepass-DB
Festplattenverschlüsselung (mobile Geräte)*

Silben-Passwort:
Bildschirm-Sperre
Online-Banking
PGP-Mail ...

Keepass generiert:
Online-Zugänge, sind auch schnell mal geändert
BIOS*
WLan, Router, Drucker, TV…

* Achtung Fallstrick: Tastaturen erzählen dem PC gerne mal was Anderes! ;-)

GMV Grundsätze digitaler Selbstverteidigung

Das Einhalten eben genannter Überlegungen bedeutet nicht,
dass keine Fehler passieren,
sie werden nur weniger.gravierend

Trotz GMV gibt es auch hier Grenzen in der Nutzung:

Die Realität zeigt: Psswörter werden nicht mehr „geknackt“,
sondern anderweitig besorgt: Comic von Munroe XKCD 538 Security

Und dieser Tage:
Gesetze gegen Hass und zur Passwortherausgabe treten in Kraft

Ausblick - andere Lösungen

Vielfalt der Möglichkeiten ist erwünscht:

geht es auch ohne Passwörter?
https://blog.medium.com/signing-in-to-medium-by-email-aacc21134fcd
Klasse Idee, wenn e2e-verschlüsselt!

Trickreiche Passwortkarte KILUG 2016
https://www.kilug.de/downloads/file/34-sichere-passw%C3%B6rter,-passwortsicherheit.html

Leben ohne Passwort - FIDO2 KILUG 2019 USB-Authenticator (Smartcard)
https://www.kilug.de/downloads/file/118-leben-ohne-passwort-fido2.html

Zugänge auf QR-Code in Tresor-Türe mit Handscanner - Idee aus dem AKIS VDI Rheingau
https://www.vdi.de/ueber-uns/vor-ort/bezirksvereine/rheingau-bezirksverein-ev/arbeitskreise

Crypto-Hardware (PGP, OTP, 2FA)

...

Was ist nun das "Best Practise" für Privatleute?

Es gibt immer noch kein automagischer Algorithmus,
nicht DAS optimale Passwort

Aber es gibt einige Hausaufgaben für die richtige Richtung:

Schritt 1: Das richtige Bewusstsein schaffen

Schritt 2: Den Passwort-Manager installieren

Schritt 3: Die Master-Kee-Pass-Phrase würfeln

Schritt 4: Die Passwort-Datenbank anlegen

Schritt 5: Die zehn wichtigsten Passwort-Einträge hinzufügen

Schritt 6: Ein Backup/Notfalldatenblatt anlegen

Schritt 7: Weitere Accounts finden und eintragen

Schritt 8: Optimieren: Browser-Procedere, Synchronisation mit anderer HW

Vielen Dank für die Aufmerksamkeit!

Wenn Ihnen der Vortrag gefallen hat: Ihre Spenden sollen an das KeePassXC-Team gehen

VDI-Konto: DE37 6805 0101 0013 3541 45

Stichwort: Spende AK-DigIT-FLUG KeePassXC

ak-digit@bv-schwarzwald.vdi.de

PGP-Key: https://keys.openpgp.org/search?q=ak-digit%40bv-schwarzwald.vdi.de

Fingerprint: 1952 732E 9F00 F41E 8C56 9543 B857 646A 8FC0 1031

Verein deutscher Ingenieure Bezirk Schwarzwald www.vdi-schwarzwald.de
Linux User Group Freiburg www.lug-freiburg.de

Copyrights, Lizenzen

https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

• Die im Vortrag benannten Produktnamen, Firmennamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

• Quellenangaben zu den verwendeten Bildern, Darstellungen etc. finden sich am Ende der Foliensammlung.

• Dieses Werk ist lizenziert unter einer CC BY-SA-ND 4.0 Lizenz
Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0

• Dieser **Vortrag ist privater Natur und verfolgt keine gewerblichen Absichten**
• Die Inhalte dienen der persönlichen Fortbildung und soll als Hilfe zur Selbsthilfe verstanden werden – eine Haftung jeglicher Art wird hiermit ausgeschlossen.

Quellenangaben

zu den Seiten:
2
https://de.wikipedia.org/wiki/Informationssicherheit#Zugangskontrolle
4
https://www.heise.de/security/meldung/Neue-Passwort-Leaks-Insgesamt-2-2-Milliarden-Accounts-betroffen-4287538.html

https://www.heise.de/security/meldung/Facebook-Hunderte-Millionen-Passwoerter-im-Klartext-gespeichert-4342184.html

Expertentipp für Linuxer:
https://www.heise.de/security/artikel/Nach-dem-Passwort-Leak-Eigene-Passwoerter-lokal-checken-4284756.html

3
nur der Zufall ist sicher!
https://digitalcourage.de/digitale-selbstverteidigung/sicherheit-beginnt-mit-starken-passwoertern

https://www.kuketz-blog.de/sicheres-passwort-waehlen-der-zufall-entscheidet/#comment-48511

https://digitalcourage.de/sites/default/files/2020-06/20200625_cryptoseminar_fh_bielefeld_web.pdf

Quellenangaben

5

KeePassXC https://keepassxc.org/docs/KeePassXC_UserGuide.html#_interface_overview

https://keepassxc.org/donate/

https://wiki.ubuntuusers.de/KeePassXC/

https://digitalcourage.de/sites/default/files/2020-06/cp_handout_KeePassXC__v1.pdf

https://www.wer-weiss-was.de/t/keepass-passwortliste-fur-windows-und-smartphone-zugriff-sicher-ablegen-und-synchron-halten/9454502/6

https://www.heise.de/ratgeber/Passwoerter-systemuebergreifend-verwalten-und-synchronisieren-mit-Keepass-5064157.html

http://www.soft-management.net/wp/2013/03/keepass-kennworteingabe-mit-auto-type/

https://keepass.info/help/kb/testform.html

https://keepass.info/plugins.html

Vertreterregelung:

Zu den klassischen Lösungsansätzen für dieses Problem gehören auf Zetteln notierte Passwörter in versiegelten Kuverts, die in einem Tresor deponiert und beim Eintreten eines Notfalls einem dazu Berechtigten ausgehändigt werden.

https://www.admin-magazin.de/Das-Heft/2013/03/Anforderungen-an-ein-zentralisiertes-Passwort-Management

Wann haben Privatleute einen absoluten Notfall?

https://www.tobias-bauer.de/files/computer/keepass-notfallblatt/KeePassNotfalldatenblatt.pdf

https://www.heise.de/forum/heise-online/Kommentare/Passwoerter-systemuebergreifend-verwalten-und-synchronisieren-mit-Keepass/Re-KeePassXC/posting-38464402/show/

Bild: https://search.creativecommons.org/photos/12817193-a49e-4975-b045-bfe2b9faa026

Quellenangaben

6

https://itsfoss.com/password-generators-linux/

https://opensource.com/article/19/11/random-passwords-bash-script

https://libredd.it/r/bash/comments/537ush/xkcd_password_generator_bash_command_works_on_a/

date | md5sum

Bild: https://search.creativecommons.org/photos/67e032f7-11ee-4679-b7b5-77d7d7c1067e

"File:Dice (typical role playing game dice).jpg" by Diacritica is licensed with CC BY-SA 3.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/3.0

7

video -> Passphrase

https://digitalcourage.video/videos/watch/911cfa32-4365-46db-b30c-71ee52628d3c

Passwort Entropie leicht erklärt: Entropie-Gleichung

https://specopssoft.com/de/blog/alles-ueber-passwort-entropie/

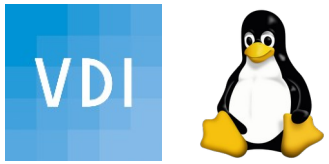
https://theworld.com/~reinhold/diceware.html

five words have an entropy of at least 64.6 bits; mittlere Org.

six words have 77.5 bits, große Org.

seven words 90.4 bits, sicher bis 2030

eight words 103 bits, sicher bis 2050



Quellenangaben

8

https://www.heise.de/ct/hotline/Linux-Passwort-vergessen-2549761.html

10

https://www.explainxkcd.com/wiki/index.php/538:_Security

https://www.heise.de/news/Gesetzespaket-gegen-Hass-und-zur-Passwortherausgabe-tritt-in-Kraft-6004554.html

11

https://ak.vdi-rheingau.de/index.php/AKIS_Arbeitskreis_Internet-Sicherheit

12 Zusammenfassung

https://www.heise.de/ratgeber/So-bringen-Sie-Ordnung-ins-Passwort-Chaos-4364704.html

13

https://www.vdi.de/ueber-uns/vor-ort/bezirksvereine/bezirksverein-schwarzwald-ev/veranstaltungen?tx_sfeventmgt_pievent%5Bcontroller%5D=Event&tx_sfeventmgt_pievent%5BoverwriteDemand%5D%5Bdistance%5D=&tx_sfeventmgt_pievent%5BoverwriteDemand%5D%5BfreeOfCharge%5D=&tx_sfeventmgt_pievent%5BoverwriteDemand%5D%5BonlyOnline%5D=&tx_sfeventmgt_pievent%5BoverwriteDemand%5D%5BworkingGroups%5D%5B0%5D=5941&tx_sfeventmgt_pievent%5BoverwriteDemand%5D%5BzipCodeCity%5D=&tx_sfeventmgt_pievent%5BsearchDemand%5D%5BendDate%5D=&tx_sfeventmgt_pievent%5Bsea

Quellenangaben

zum weiter stöbern...

Vorbereitung: https://yopad.eu/p/Flug-VDI-365days

Nachlese: http://lug-freiburg.de/pages/projekte.html

https://help.gnome.org/users/seahorse/stable/index.html.de

https://www.heise.de/forum/c-t/Kommentare-zu-c-t-Artikeln/Festplattenverschluesselung-mit-Brute-Force-knacken/Re-Richtiges-Passwort-in-der-History/posting-36851885/show/

https://www.heise.de/forum/c-t/Kommentare-zu-c-t-Artikeln/Festplattenverschluesselung-mit-Brute-Force-knacken/Re-Frau-Marky-richtiges-Passwort-wird-nicht-erkennt/posting-36850840/show/

https://www.heise.de/security/artikel/Nach-dem-Passwort-Leak-Eigene-Passwoerter-lokal-checken-4284756.htm
l

https://www.heise.de/forum/heise-online/Kommentare/Passwoerter-systemuebergreifend-verwalten-und-synchronisieren-mit-Keepass/Re-KeePassXC/posting-38464402/show/

https://www.heise.de/forum/heise-online/Kommentare/Passwoerter-systemuebergreifend-verwalten-und-synchronisieren-mit-Keepass/Tipp-Syncthing-KeepassXC/posting-38510755/show/

Vermutlich kein Hack, sondern Phishing...

Nur, dass ich mir ein komplexes Passwort mit 20 Stellen nicht merken kann, einen Satz aus 8 Wörtern aber schon eher...