Persönliche Sicherheit & Datenschutz mit Passwortmanager

Tux-Tage
2021Nov14 @ 09:00
jitsi

der.hans (https://floss.social/@FLOX_advocate)
CDE Manager
Object Rocket, a rackspace company
https://www.ObjectRocket.com/

Ja, wir stellen ein :)

Rackspace Technologies
https://rackspace.jobs/careers/?location=null&search=germany

griaßle

Figure 1. Aaron Swartz Day

https://www.aaronswartzday.org/

Kommende Vorträge

- GeekBeacon Fest - https://www.gbfest.org/
  - Fediverse: Decentralized Social Networking and Services
  - nach Februar verschoben
- liste meine Vorträge und wo die heutige Slide eventuell zu finden
  - https://www.LuftHans.com/talks

Aller Erste

IBKR

Und

ausdrücklich…

Noch Wichtiger!

IBDRN

Wenn Du irgendwelche Rechtsberatung brauchst, setzt Dich in Verbinding mit Deinem eigenen Rechtswanwalt

GDPR

mit GDPR ist unser Begriff auf unsere eigene Dataien verbessert

es soll auch weniger von unserer persönlicher Infos von Firmen gespeichert

Firmen haben aber nicht Plötzlich bessere Sicherheit

Wieso brauchen wir die Eigene Sicherheit?

Spectre/Meltdown (noch wieder)

— FRITZed — Heartbleed — Apple SSL — Apple iCloud — Yahoo! x 2 — LinkedIn x 3 — Eharmony — Last.FM — Adobe

— Mat Honan — Jennifer Lawrence — Kate Upton — Rhianna

Der wahre Risiko

> "They could have used my e-mail accounts to gain access to my online banking, or financial services. They could have used them to contact other people, and socially engineer them as well." – Mat Honan

Was ist eigentlich zu verlieren?

> "more than a year’s worth of photos, covering the entire lifespan of my daughter" – Mat Honan

> "including those irreplaceable pictures of my family, of my child’s first year and relatives who have now passed from this life" – Mat Honan

Dateien Saugen

- 90% alle bekannte Dateien wurden in der letzte 2 Jahren gesammelt
    - aus eine 2019 Freakanomics Podcast

Ganz Wichtig!

- Patchen!
- Nur von verträuliche Softwarequellen!

Verschlüßelungsbeispiel

- Postkarte v. Briefumschlag

Wann soll man Verschlüßelung benutzen?

- Immer :)
- Jedes Mal
- HTTPS Everywhere vom EFF

Was soll man verschlüßeln?

- Beschienigungen
- Persönliche (identifizeriende) Infos
    - Name
    - Anschrift
    - Telefonnummer
    - EC Karte Infos
    - Gesundheitsinformation
    - Privatfotos
    - Schuhgroße

Password Bleedover

- Gleiche Passwort bei viele Domänen?
- Einbrechung bei einer kann schnell Einbruch bei Alle werden
- Benutze einzigartige Passwörte bei jedem Dienstanbieter

Bescheinigung für Zugang

- Bescheinigungen sind nich nur Nutzernamen u Kennwörter

Bist Du Du?

- Benutzername, oft Emailanschrift
- Passwort
- Sicherheitsfragen und -antworten
- Multifakter Authentizierung (MFA)
- Körperteil

Einzigartige Beschienigungen

- jeder Teil soll einzigartig für jeder Site
- jeder Teil, nicht nur als Ganze
- gewisse Einschränkungen gelten

Random String / zufallsbedingt Zeichenskette

- unerkennbare Zeichenssalat
- je längere und zufälligere Ketten desto besser
- benutze
    - alphabetische Buchstaben
    - Nummern
    - Satzzeichen (`!@#$%^&*.,/:\;`)
- Acht auf
    - gleichaussehenede Zeichen Falls man es tippen oder aussprechen muss
    - Unterstreichen und Ergänzungsstrich
    - Leertasten und Tabulator
- Kettenbeispiel: `fnYV@tki4M’jj;iTW]21`

Wortsalat

- unsinnige Wortsequenz
- je längere und zufälligere Wortketten desto besser
- Wörter aus mehrere Sprachen
- Deklination u Konjugation
- großbuchStaben iM woRt
- zufällige Satzzeichen
- Beispiel: purplish Leche verFaehrt singing liberte
- bekannte XKCD Beispiel: correct battery horse staple

Hilfe, da spinne ich …

Aber, Hans, es ist viel zu viel um auswendig zu lernen und nicht Mal so Interessant wie kernel debug logs …

Password Managers / Passwortverwalter

- Beschienigungsinfos sicher speichern
- sehr einfach zu nutzen

Passwortverwalter Anforderungen

- freier Software
- verborgene Passwörter
- lokal Verschlüßelt
- Operating System unabhängige Akte
- Dateien Freisetzung
- Zwischenspiecher automatisch löschen
- einfache kopieren und einfügen
- konfigurbare Passwortgenerator
- Notizen

Passwortverwalter Bonusrund

- lesbare und sprechbare Passwortgeneration
- zufallsbedingt Wort generation
- Sprachhinweise
- zufallsbedingt Zeichenskettegenerator immer zugriffbar
- Datenexportieren mit Sync

meine Empfehlungen

- GNU/Linux or BSD Device
  - KeePassXC (keepassxc-cli)
  - KeePassX, version 2.x (kpcli)
- Web
  - BitWarden
  - Nextcloud
    - WebAppPassword
    - Passman
    - Passwords
- Android
  - KeePassDroid
- andere Betriebssysteme
  - KeePass

Ein Passwort um die Alle zu behalten

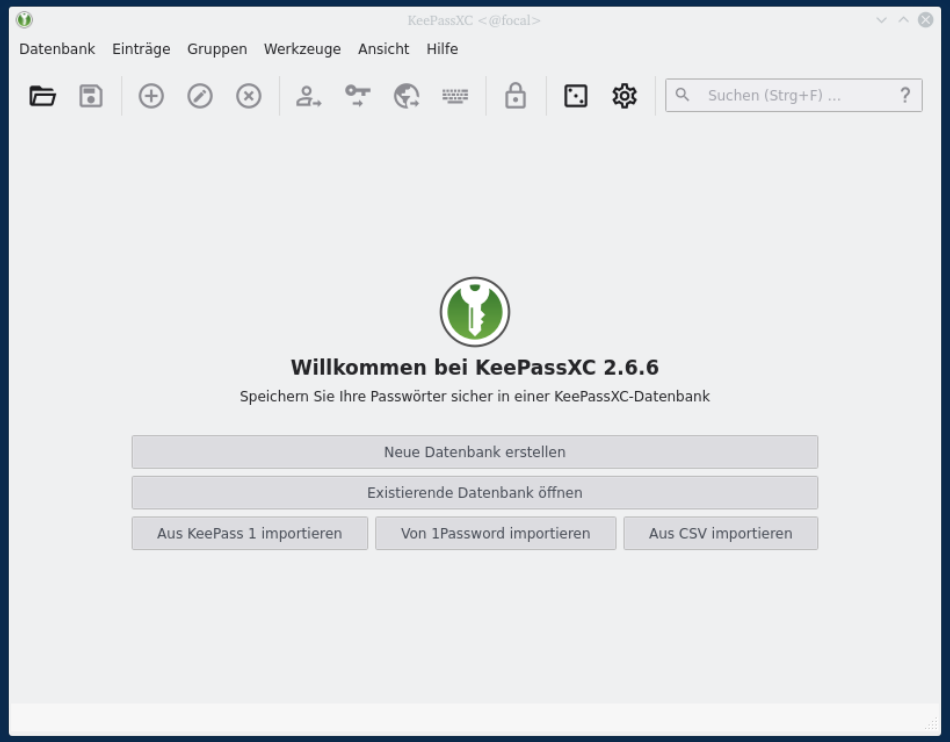
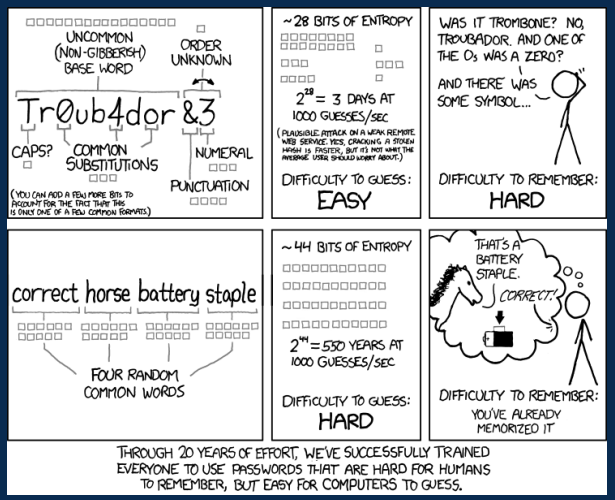


Figure 2. Willkommen bei KeePassXC

Ein Passwort um die Alle zu schutzen

Passphrases



XKCD: Password Strength - https://xkcd.com/936/

aussprechende Zeichensketten

- nutzbar für’s Telefonierung
- Vorsicht gleichaussehende Zeichen
  - 1 l
  - 0 O
- Sprachhinweise
  - werecbyivofejmu (wer-ec-byiv-of-ej-mu)

Ich bin Ich!

Authentifikation stellt sicher, daß Du Du bist

Wie kann man es beweisen?

- 3 Arten Beschienigungsinfos
  - Was weißt Du?
    - Username, Passwort, PIN
  - Was hast Du?
    - Ausweis, Handy, Token
  - Was bist Du?
    - Fingerabdruck, DNA, Gesichtserkennung
      - https://reclaimyourface.eu/

4. Art: Token

- Browserkeks
- Handy Device ID

ID: Username

- Womöglich, zufällige Zeichensketten benutzen
  - zB: Bank, Einkaufen, usw
  - Ex: `eddyityoz`
- zufällige Zeichensketten sind für Social Network nicht geeignet
- erkennbare Name: öffentliche und gesellschäftliche Sites
  - Es: `FLOX_advocate`

ID: Emailanschrift

- Subaddressing
  - `username@gmail.com`
  - `username+randomstring@gmail.com`
- Super bei Mailfiltern
  - `username+3qkrl-ebay@gmail.com`
- beschränte Nutzligkeit bei Socialmedia
  - Freunde und Kollegen
    - `username@gmail.com ist Bekannte von Mir`
  - Socialmedia Benachrichtungen
    - `username+mastodon@pm.me`

ID: Verwendung von Subaddressing

- zufällige Emailanschrift bie jeder Dienstanbieter
- benutze zufällige Zeichensketten für Subaddressing
  - mit Sitename nach der Zeichenssalat
    - `username+3qkrl-ebay@gmail.com`
      - Benutzername: `username`
      - Token: `3qkrl`
      - Site: `ebay`
- Bonus
  - Filter Email für die Anschrift
  - Spamerkennung

ID: Keks

- Dritte Partei Keks verfolgen uns auf mehrere Domänen
- Lightbeam 3.0 Add-on
- uMatrix Add-on

ID: Sicherheits Fragen und Antworten

Das wichtigste dabei ist…

Unsinn ist sicherer

IBKR

Noch eine kurze Errinerung dran, IBDRN

In den USA können wir schon um Sicherheitsantworten und zum Teil auch bei Geburtsdatum lügen

In der EU, bin ich mir nicht sicher …

ID: Sicherheits Fragen und Antworten

- zufällige Antworten
- zufällige Wortsalat als Fragen
- aussprechbare Wort- und Zeichensketten

ID: Multifakter Authentizieren (MFA)

- TOTP - Time-Based Tokens
- HOTP - HMAC
- Message - SMS
- Message - Schiebnotifikation
- Telefonanruf
- Email
- Körperteil

MFA: TOTP (Applikation or Token)

- Zeit basierte Token
- Dientsanbieter brauchen Deine Telefonnummer nicht
- Handy oder Tablet wie Token benutzen
- meine Empfehlung

MFA: HOTP

- Jede Ziffer kann nur ein Mal benutzt werden

MFA: braucht Handynummer

- SMS
  - MitM
  - verlorene Handy
- Message - Schiebbenachrichtigung
- Anrufe
  - Sehe SMS :)

MFA: Email

- Sehe SMS :)
  - Lieber Spam als Verkaufsanrufe

MFA: Körperteil

- schwer zu ändern (bis wir Cyborge werden)

ID: Geburtsdatum

- Lüg wenn möglich
- 31. February funz nimmer :(
- One-liner für zufällige Datum zwischen 1954 und 1999

```
- date -d @$RANDOM*24*3600/2-500000000 +%Y%b%d
```

ID: PINs

- dürfen manchmal bis sechsstelliger Zahlenkode

Backups

- regelmäßige Backups
- offsite Backups
- Löschen
    - Clouds are forever / Datenwolkenanbieter sind für immer

Nicht Vergessen!

Eindeutige Beschienigungsinfos für jeden Dienstanbieter!

die Wahrheit

soziale Medien und Fediverse

- FLOX_advocate auf Mastodon
  - https://floss.social/@FLOX_advocate
- LuftHans auf ~~Freenode~~ Libera.chat IRC
  - #SeaGL, #LOPSA, #PLUGaz and #LibreLounge

Glossary

- Credentials
  - Anything used to identify you for authentication
- Passphrases vs passwords
  - Essentially the same
  - passphrases implies they are longer and the ability to use special characters and spaces
- Subaddressing delimiters
  - Often a '+', but doesn’t have to be. Depends on your mail provider.

Quellen

- Linux Journal (2017Jan): Online Privacy and Security Using a Password Manager
  - https://www.LuftHans.com/LinuxJournal/Online_Privacy_and_Security_Using_a_Password_Manager
- My talks and publications
  - https://www.LuftHans.com/talks/
- Mat Honan Wired article
  - http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- Subaddressing list at Wikipedia
  - http://en.wikipedia.org/wiki/Email_address#Address_tags
- XKCD "Password Strength" explained
  - https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength
- Nextcloud Video Verification
  - https://nextcloud.com/blog/unique-sharing-security-video-verification/

Obtaining Software

- KeePassXC
  - https://KeePassXC.org/
- KeePassX
  - https://www.KeePassX.org/
- FDroid
  - https://f-droid.net/
- Bitwarden
  - https://bitwarden.com/
- Nextcloud
  - https://Nextcloud.com/
    - WebAppPassword
    - Passman
    - Passwords

Privacy Enhancing Firefox Add-ons

- https://addons.mozilla.org/en-US/firefox/addon/umatrix/ [uMatrix] from https://addons.mozilla.org/en-US/firefox/user/11423598/ [Raymond Hill]
- https://addons.mozilla.org/en-US/firefox/addon/noscript/ [NoScript] from https://addons.mozilla.org/en-US/firefox/user/143/ [Giorgio Maone]
- https://addons.mozilla.org/en-US/firefox/addon/lightbeam-3-0 [Lightbeam 3.0] from https://addons.mozilla.org/en-US/firefox/user/15365629/ [Princiya]
    - forked from Mozilla by former Outreachy intern in Berlin
- https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/ [uBlock Origin] from https://addons.mozilla.org/en-US/firefox/user/11423598/ [Raymond Hill]
- https://addons.mozilla.org/en-US/firefox/addon/ubo-scope/ [uBO-Scope] from https://addons.mozilla.org/en-US/firefox/user/11423598/ [Raymond Hill]

Credits

- XKCD by Randall Munroe
  - http://XKCD.com
  - Password Strength - https://xkcd.com/936/
- Freakonomics Radio
  - America’s Math Curriculum Doesn’t Add Up (Ep. 391)

Bonus Rounds

Data Escrow

- Use a KeePassXC file to store other important information
  - Bank account info
  - Life insurance info
  - Government citizen numbers
  - Passphrases for GPG keys
  - PDF copies of contracts and other documents
  - Use multiple different files

Tips

- Don’t use links in email to login
- Use application-specific passwords
- Don’t use Internet Explorer
- Don’t use Outlook

Getting Help

- Tech Support Fastlane - http://xkcd.com/806/
- Free Software Conferences (Tux-Tage, Kielux, CLT, FOSSASIA, SeaGL, SCaLE)
- Local user groups