persönliche Sicherheit und Datenschutz durch ein Passwortverwalter

der.hans - https://www.LuftHans.com/talks/

2018Jun09 @ Tübix

Aller Erste

IBKR

Und

ausdrücklich…

Noch Wichtiger!

IBERN

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

GDPR

mit GDPR ist unser Begriff auf unsere Eigene Dataien verbessert

es soll auch weniger persönliche Infos von Firmen gespeichert

Firmen haben aber nicht Plötzlich bessere Sicherheit

Warum brauchen wir die Eigene Sicherheit?

Spectre/Meltdown — FRITZed — Heartbleed — Apple SSL — Apple iCloud — Home Depot — Target — Yahoo! x 2 — LinkedIn x 3 — Eharmony — Last.FM — TJ Maxx / Marshalls — Adobe — Nieman Marcus — 7-eleven — Barnes and Noble — TriCare x 2 — Mat Honan — Jennifer Lawrence — Kate Upton — Rhianna

Cost

> "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

What’s at Stake

> "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

Ganz Wichtig!

- Patchen!
- Nur verträuliche Softwarequellen!

Verschlüßelungsbeispiel

- Postkarte v. Briefumschlag

Wann soll man Verschlüßelung benutzen?

- Immer :)
- HTTPS Everywhere
  - Jetzt von Firefox add-ons erhältbar

Was soll man verschlüßeln?

- Beschienigungen
- Persönliche Infos
  - Name
  - Anschrift
  - Telefonnummer
  - EC Karte Infos
  - medische Infos
  - Privatfotos
  - Schuhgroße

Password Bleedover

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

Hilfe, da spinne ich…

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

Password Managers / Passwortverwalter

- Beschienigungsinfos sicher speichern
- sehr einfach zu nutzen

Passwortverwalter Anforderungen

- freier Software
- lokale Verschlüßelt
- Operating System unabhängige Akte
- verborgene Passwörter
- Zwischenspiecher automatisch löschen
- Daten Liberation
- einfache kopieren und einfügen
- konfigurbare Passwortgenerator
- Notizen

Passwortverwalter Bonusrund

- lesbare und sprechbare Passwortgeneration
- Sprachhinweise
- zufallsbedingt Wort generation, aka Diceware
- zufallsbedingt Zeichenskette generation immer zugriffbar
- Datenexportieren mit Sync

meine Empfehlungen

- KeePassXC
- KeePassX, version 2.x
- KeePassDroid
- keepassxc-cli or kpcli
- KeePass

Random String / zufallsbedingt Zeichenskette

- unerkennbare Zeichenssalat
- längere und zufälligere Ketten sind besser
- alphabetische Buchstaben
- Nummern
- Punktuation `(  !@#$%^&*.,/:\; )`
- acht auf gleichaussehenede Zeichen Falls man es tippen oder aussprechen muss
- Kettenbeispiel: `fnYV@tki4M'jj;iTW]21`

Diceware

- Vier oder mehr unverbundene Wörter
- Suche Mal "xkcd correct horse battery staple"

Ein Passwort um die Alle zu behalten

aussprechende Zeichensketten

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

Bist Du Du?

Authentifikation stellt sicher, daß Du Du bist

Wie kann man es beweisen?

- 3 Arten Beschienigungsinfos
  - Was weißt Du?
    - Username, Passwort, PIN
  - Was hast Du?
    - ID, Handy, Token
  - Was bist Du?
    - Fingerabdruck, DNA

Token

- Browserkeks
- Handy Device ID

Bescheinigungsinfos

- Username: oft Emailanschrift
- Passwort
- Sicherheits Fragen und Antworten
- Multifakter Authentizierung (MFA)
- Geburtsdatum
- PIN

ID: Username

- Womöglich, zufällige Zeichensketten benutzen
  - Wie erkennt Dir das Geschäft?
  - Bank, Einkaufen, usw
- zufällige Zeichensketten funzen bei Social Network nicht
  - Wie erkennt Dir andere Leute?

ID: Emailanschrift

- Subaddressing
  - username@gmail.com
  - username+randomstring@gmail.com
- Super für filtern
  - username+3qkrl-ebay@gmail.com

ID: Using Subaddressing

- zufällige Emailanschrift bie jeder Dienstanbieter
- benutze zufällige Zeichensketten für Subaddressing
  - mit Sitename nach der Zeichenssalat
- Bonus
  - Filter Email für die Anschrift
  - Spamerkennung

ID: Keks

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

ID: Sicherheits Fragen und Antworten

Das wichtigste dabei ist…

Nonsense Is More Secure

Lüge!

IBKR

Noch eine kurze Erringerung, IBERN

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

In der EU, weiß ich nicht…

ID: Sicherheits Fragen und Antworten

- zufällige Antworten
- zufällige Zeichensketten
- aussprechbare Zeichensketten

Multifakter Authentizieren (MFA)

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

MFA: TOTP (Applikation or Token)

- Dientsanbieter brauch Deine Telefonnummer nicht
- Zeit basierte Token
- Handy oder Tablet wie Token benutzen

MFA: HOTP

- Jede Ziffer kann nur ein Mal benutzt

MFA: Message - SMS

- Basiert auf Handynummer
- MitM
- MFA - verlorene Handy

MFA: Message - Schiebnotifikation

- Handy braucht Internetzanschluß

MFA: Email

- Sehe SMS :)
  - Lieber Spam als Verkaufsanrufe

MFA: Anrufe

- Sehe SMS :)

MFA: Körperteil

- schwer zu ändern bis wir Cyborg werden

ID: Geburtsdatum

- Lüge wenn möglich
- February 31 funz nimmer :(
- One-liner für zufällige Datum
  - `date -d @$((RANDOM*24*3600/2-500000000)) +%Y%b%d`

Andere Infos

- Dienstanbieter Passwort Begrenzungen
- angefordete Keks und JavaScript

Backups

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

Nicht Vergessen!

Eindeutige Beschienigungsinfos für jeden Dienstanbieter!

Contacting Hans

Danke Schön!

- https://mastodon.social/@lufthans
  - Mastodon
- https://plus.google.com/106398898073454924098
  - G+
- LuftHans on Freenode, usually in #LOPSA and #PLUGaz
  - IRC

Resources

- Credentials
  - Anything used to identify you as you to a system for authentication
- Passphrases vs passwords
  - Essentially the same, but 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.

Resources

- Linux Journal (2017Jan): Online Privacy and Security Using a Password Manager
- Previous talks: http://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
- Discussion of Password Strength XKCD
  - http://www.explainxkcd.com/2011/08/10/password-strength/

Obtaining Software

- KeePassXC
  - https://keepassxc.org/
- EFF’s HTTPS Everywhere
  - https://www.eff.org/https-everywhere/

Credits

- XKCD by Randall Munroe
- http://XKCD.com
- Domino image
- https://openclipart.org/detail/193062/falling-dominoes-by-mazeo-193062

Bonus Rounds

Data Escrow

- Use a KeePassXC file to store other important information
  - Bank account info
  - Life insurance info
  - SSNs
  - Passphrases for GPG keys
  - 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/
- Local user groups