# Digitale Selbstverteidigung

(Weißer Gürtel)

Vorweg:

Wir sind keine Experten und wollen an dieser Stelle keine Fachdiskurse erörtern, sondern Grundsätzliches vermitteln, um das allgemeine Bewusstsein und den Standard im Umgang mit sensiblen Daten zu verbessern.

# Wie werden Daten gesammelt?

# Wie werden Daten gesammelt?

- (Internet) Service Provider speichern Verbindungsdaten auf Vorrat
- Webdienste* identifizieren Nutzer*innen über
  - Geräte-ID
  - Software-Hardware-Fingerabdruck
  - Cookies
  - IP-Adresse
  - Loginstatus bei Diensten wie Google / Facebook
- Webdienste schneiden Bewegungen und Verweildauer mit
- Eingaben und Interaktionen (Einkaufen, “Likes” usw.) werden gespeichert
- freigegebene Daten (Kontakte, Mikrofon, Kamera) werden ausgelesen
- Daten werden bei ungeschützter Übertragung abgefangen

* Websites, Suchmaschinen, Apps, Software, ...

# Wie werden Daten gesammelt?

- mobile Geräte können via WLAN / GPS / Bluetooth sehr genau geortet werden, bspw. in Läden
- Daten aus verschiedenen Quellen werden zusammengetragen, Nutzer*innen-Profile angelegt
- Daten werden weiterverkauft und aus anderen Quellen eingekauft

# Wer sammelt meine Daten?

# Unternehmen

- Datensammeln gehört häufig zum Businessmodell
- kaufen und verkaufen Daten
- legen anhand der Daten Ratings an (Kredit, Gesundheit) [1][2]
- haben politische Interessen, arbeiten mit Staaten und beeinflussen Politik
- erstellen anhand von großen Datenmengen Prognosen für (Finanz-)Produkte und Ökonomien

# Webdienste, Apps

- Ziel: Nutzungszeit / Interaktionsrate maximieren [3]
- legen Nutzer*innen-Profile an und speisen Algorithmen [4]
- personalisieren Werbung und Inhalte

# Staaten, Behörden, Geheimdienste

- Überwachung (“Staatstrojaner”)
- Strafverfolgung
- politische Einflussnahme [5][6]
- Verwaltung [7]
- Risikobewertung [8][9]

# Negativfolgen

- Werbung (die funktioniert)
- ein Leben in der Filterblase
- kein Kredit
- Wohnung ciao
- Versicherung teuer
- Knast für dich und alle deine Freund*innen
- Online-Sucht [10]
- finanzieller und psychischer Ruin [11]
- “Anbieter*innen-freundliche” Normierung von Verhalten und “Netzarchitektur”
- ein Algorithmus ist mehr oder minder eine Blackbox

# Black Hat Hacker (auch staatlich)

- interessieren sich nicht für Recht und Ethik
- fangen Daten ab oder verschaffen sich Zugriff
- knacken von Webdiensten gespeicherte Daten
- Betrug, Erpressung, Diebstahl
- Stalking, Doxxing
- nutzen fremde Geräte für Botnetze
- verkaufen Daten

Anhand der über dich gesammelten Daten wird dein Leben beeinflusst, ohne dass du es weißt oder dich dagegen wehrst.

Andere haben auch Interesse an den Daten, die du nicht freiwillig preisgibst.

Deine Daten sind auch Daten über deine Freund*innen.

Wer sammelt meine Daten?

# Wer auch immer es will.

# Worauf kann ich achten?

# Nutzungsverhalten

- sich im Klaren sein, dass alle Daten grundsätzlich mitgeschnitten oder entwendet werden können
- Apps und Dienste meiden, die Daten sammeln / verkaufen
- Suchmaschine wechseln (z.B. *DuckDuckGo* statt *Google*) [12]
- Open-Source-Software bevorzugen (z.B. mit *Firefox* browsen) [13]
- bei Apps aufpassen, welche Berechtigungen verlangt werden (Mikrofon, Adressbuch, W-LAN)

# Nutzungsverhalten

Sicherer browsen mit (vertrauenswürdigen) Addons:

- *uBlock* (nicht *adblock*) [14]
- *Privacy Badger* [15], ~~*Ghostery*~~ [16], *Disconnect.me* [17]
- *HTTPS Everywhere* [18]

# Nutzungsverhalten

Geräte haben eine ID bzw. hinterlassen einen digitalen Fingerabdruck

- WLAN / GPS / Bluetooth im Smartphone nur aktivieren, wenn benötigt (senden Geräte ID)
- Smartphone ausschalten oder Zuhause lassen, wenn’s wichtig wird

# Nutzungsverhalten

Smart-(Home-)Devices meiden

- hören quasi immer mit
- Daten werden gesammelt, verwertet, verkauft
- Polizei kann Zugriff verlangen
- zumindest open source nutzen [19]

# Nutzungsverhalten

Nicht alle wichtigen Daten an einem Punkt zusammenlaufen lassen:

- verschiedene Mails für verschiedene Dienste verwenden
- unterschiedliche Geräte / Browser für verschiedene Aktivitäten
- verschiedene Datenträger für verschiedene Daten
- kein Universalpasswort verwenden

# Nutzungsverhalten

- umsichtig mit Aufnahmen umgehen
- Kameras abkleben
- Dummy Plugs benutzen
- Daten sicher löschen

# Sichere Kommunikation

- verschlüsselte Messaging-Apps verwenden (z.B. *Signal*) [20]
- vertrauenswürdige Mailprovider (z.B. *Riseup* [21], *Posteo* [22] hat aber Server in DE)
- Mailverkehr verschlüsseln mit PGP (z.B. *Enigmail* für *Thunderbird*) [23]
- Virtual Private Network (VPN) nutzen, um Webverkehr zu verschleiern
  - auch hier einen vertrauenswürdigen Dienst wählen (anonym, sicher vor staatl. Zugriff)
- *TOR-Browser* nutzen [24]

# Daten schützen

- Geräte / Programme passwort-sichern
- richtige Passwörter (Plural!) benutzen (und sonst nichts)
- ggf. Passwörter von Logins ab und zu ändern [25]
- 2-Faktor-Authentifizierung einrichten (z.B. *Authy*, leider nicht os) [26]
- Passwort-Management (z.B. *KeePass*) [27]
- Datenträger verschlüsseln (z.B. *VeraCrypt*) [28]
- Vor wem schütze ich mich? Online-Zugriff oder Hausdurchsuchung?

# Konkrete Maßnahmen:

1. Mitdenken
2. Verschlüsselter Messenger: **Signal**
3. Browser: **Firefox** mit folgenden Addons: **uBlock**, **Privacy Badger**, **HTTPS Everywhere**… oder im Zweifel: TOR-Browser
4. Mail: **Thunderbird** mit Addon **Enigmail** für PGP-Verschlüsselung
5. Suchmaschine: **DuckDuckGo**
6. Passwörter managen mit **KeePass**
7. Datenträger verschlüsseln: **VeraCrypt**
8. ein Virtual Private Network (**VPN**) nutzen, z.B. *NordVPN*
9. ein Live-Betriebssystem wie **Tails** benutzen

# Lesetipps

- Systemli.org / https://www.systemli.org/index.html
- Netzpolitik / https://netzpolitik.org
- Capulcu / https://capulcu.blackblogs.org
- Electronic Frontier Foundation / https://www.eff.org/about

# Verweise


[1] https://www.naic.org/cipr_topics/topic_big_data.htm

[2] https://www.bigdatascoring.com/

[3] http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/

[4] https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2018/10/Disrupt2018-11web.pdf

[5] https://journals.sagepub.com/doi/10.1177/2053951718811844

[6] http://www.philosophyofinformation.net/wp-content/uploads/sites/89/2017/06/Brazil-Ready.pdf

[7] https://www.researchgate.net/publication/320689065_Big_Data_and_E-government_A_review

# Verweise


[8] https://journals.sagepub.com/doi/abs/10.1177/0003122417725865/

[9] https://non.copyriot.com/die-logik-und-die-politik-der-praevention/

[10] http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/

[11] https://theatlantic.com/.../has-the-smartphone-destroyed-a-generation/534198/

[12] https://duckduckgo.com

[13] https://www.mozilla.org/de/firefox/new/

[14] https://ublock.org

# Verweise


[15] https://www.eff.org/privacybadger

[16] https://www.ghostery.com/de/

[17] https://disconnect.me

[18] https://www.eff.org/https-everywhere

[19] https://opensource.com/tools/home-automation

[20] https://www.signal.org/de/

[21] https://riseup.net

# Verweise

[22] https://posteo.de/de

[23] https://www.enigmail.net/index.php/en/

[24] https://www.torproject.org/download/

[25] https://haveibeenpwned.com

[26] https://authy.com

[27] https://keepass.info

[28] https://www.veracrypt.fr/en/Downloads.html