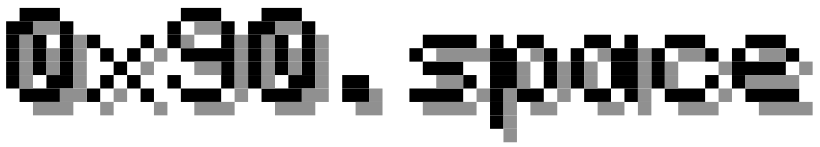
# Datenschutz

panda & vmann

# Inhalt

- Was ist Datenschutz?
- Wer interessiert sich für meine Daten?
- Warum sollte ich Daten schützen?
- Wie schütze ich mich und andere?

# Wer wir sind




Wir sind eine kleine Hackgruppe in Nürnberg, die entsprechend unseres Namens ("nop-space”) nichts tut.

Manchmal scheitern wir beim Nichtstun. Dann machen wir auch Projekte oder geben Workshops.

Vmann:

(Fach-) Idiot

Panda:

War mal in einer Partei die sich für Datenschutz eingesetzt hat, ist dann in ein Informatikstudium reingerutscht und irgendwie im Master angekommen.

# Was ist Datenschutz?

- personenbezogene Daten:
  - “alle Informationen, die sich auf eine [...] identifizierbare natürliche Person beziehen”*
- identifizierbar
  - “direkt oder indirekt”*
  - Zuordnung zu einer Kennung, Kennnummer, Merkmal, Standortdaten u.ä.*

* Art. 4 Abs. 1 DSGVO

# Was ist Datenschutz?

- Alex

## Beispiele: Personenbezogene Daten

| | | | |
|---|---|---|---|
| Geburtstag<br>18.02.99 | hat am Montag um 10 Uhr bei Rewe veganen Pudding gekauft | hat heute Nacht um 2 Uhr Avengers: Endgame gestreamed | wohnt innerhalb der Postleitzahl<br>90439 |
| besucht regelmäßig die Website<br>`zeit.de` | ist Mitglied der Facebook-Gruppe<br>`FAU Studenten` | Kontostand:<br>498 € | hat gestern um 20 Uhr nach<br>`Bitcoin ohne Ausweis kaufen`<br>gesucht |

# Was ist Datenschutz?

- Alex

# Was ist Datenschutz?

- Alex
- ID: 123-456-7890

# Was ist Datenschutz?

- Alex
- ID: 123-456-7890
- Person mit seltenen Krankheit wohnhaft in Bayern

# Was ist Datenschutz?

- Alex
- ID: 123-456-7890
- Person mit seltenen Krankheit wohnhaft in Bayern
- usw.

# Was ist Datenschutz?

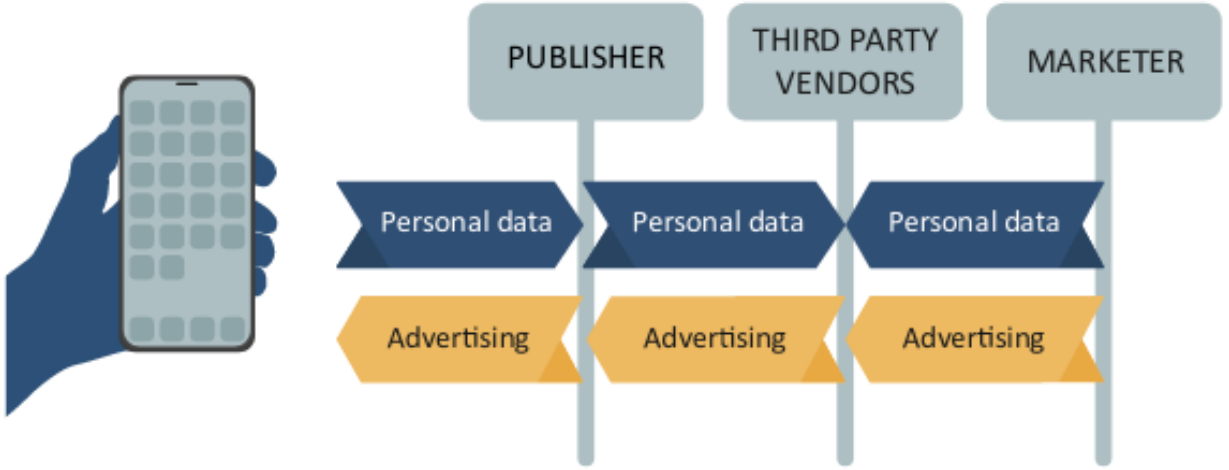
- Alex
- ID: 123-456-7890
- Person mit seltenen Krankheit wohnhaft in Bayern
- usw.

**Allgemein:**
**Personenbezogene Daten zu besitzen bedeutet eine gewisse Macht zu besitzen.**

# Wer?

- Unternehmen (Werbung, Scoring, Analytics, …)
- Staat
- Scammer / Stalker / …
- Forschung

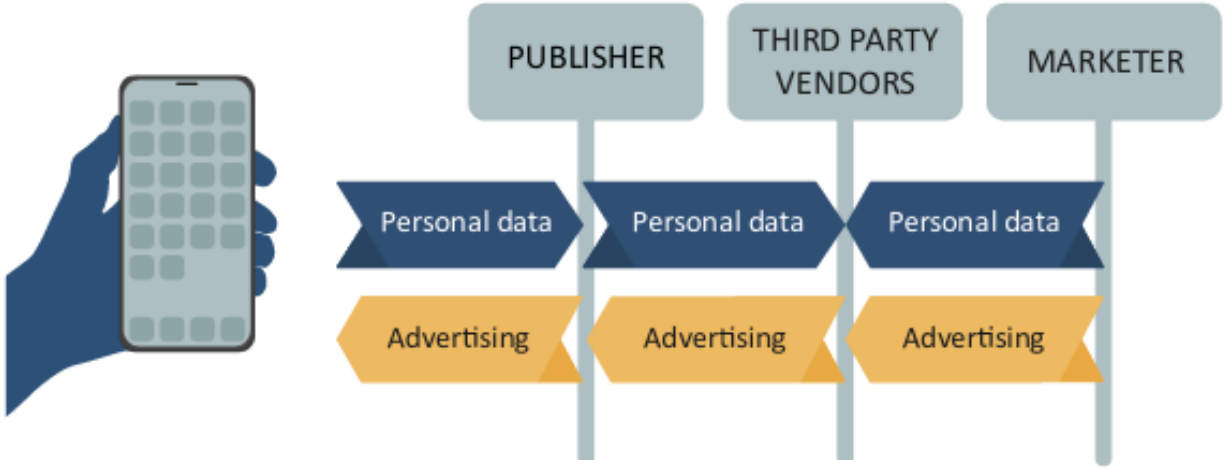
# Personalisierte Werbung



*

* Abb. aus “Out of Control” (Forbrukerrådet, 2020).
** Abb. aus “Technical Report: Out of Control” (mnemonic, 2020).

# Personalisierte Werbung




*

**


```
{
  "sdk_version": "PlacerSDK 2.7.11.1",
  "data": [
    {
      "type": "location",
      "time": "2019-07-16T11:53:35.953+0200",
      "serial": 0,
      "session_serial": 0,
      "value": {
        "provider": "fused",
        "time": "2019-07-16T11:53:35.482+0200"
        "accuracy": 15.956999778747559,
        "loc": {
          "long": 6.redacted,
          "lat": 62.redacted
        },
```


**


```
{
  "type": "wifi_info",
  "time": "2019-07-16T11:53:35.869+0200",
  "serial": 0,
  "session_serial": 0,
  "value": {
    "WifiState": "On",
    "wifi_active_network": {
      "SSID": "\"testnetwork\"",
      "BSSID": "36:16:XX:XX:XX:XX",
      "RSSI": -52
    },
```


* Abb. aus “Out of Control” (Forbrukerrådet, 2020).

** Abb. aus “Technical Report: Out of Control” (mnemonic, 2020).

# Personalisierte Werbung

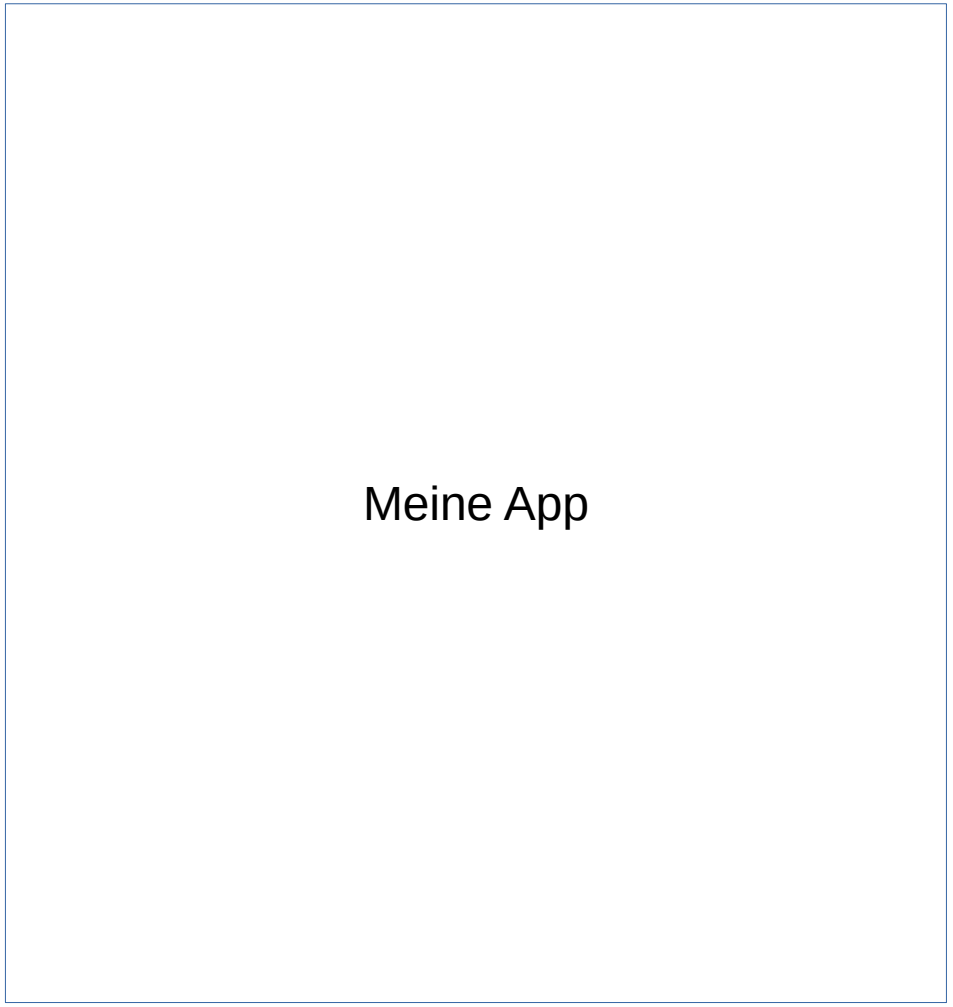
| App | Summary of findings |
|---|---|
| Clue | Sends birth year to **Amplitude**, **Apptimize**, and **Braze**.<br>Sends Advertising ID to **Adjust**, **Amplitude**, and **Facebook**. |
| Grindr | Sends GPS coordinates to **AdColony**, **Braze**, **Bucksense**, **MoPub**, **OpenX**, **Smaato**, **PubNative**, **Vungle**, and others. Sends the IP address to **AppNexus** and **Bucksense**, and information about "relationship type" to **Braze**.<br>Sends Advertising ID to all of these third parties and others, except **Braze.** |
| Happn | Sends country, gender and age segment of the user to **Google**.<br>Sends Advertising ID to **Adjust** and **Facebook**. |
| Muslim: Qibla Finder | Sends IP address to **Appodeal**.<br>Sends Advertising ID to **AppLovin**, **Appodeal**, **Facebook**, and **Liftoff**. |
| My days | Sends GPS coordinates and Wi-Fi access point information to **Neura**, **Placed**, and **Placer**. Sends IP address and a list of installed apps on the phone to **Placed**. Sends Advertising ID to **AppLovin**, **Liftoff**, **Google**, **Ogury Presage**, and **Placed**. |
| My Talking Tom 2 | Sends IP address to **Mobfox**, **PubNative**, and **Rubicon Project**.<br>Sends Advertising ID to **AppsFlyer**, **AppLovin**, **Facebook**, **IQzone**, **ironSource**, **Mobfox**, **Outfit7**, and **Rubicon Project**. |
| OkCupid | Sends GPS coordinates and answers to personal questions to **Braze**. Sends detailed device information to **AppsFlyer**. Sends Advertising ID to **AppsFlyer**, **Facebook** and **Kochava**. |
| Perfect365 | Sends various location data such as GPS coordinates and Wi-Fi access point information to **Fysical**, **Safegraph**, and **Vungle**. Sends GPS coordinates unencrypted to **Receptiv**. Sends Advertising ID to **Amazon**, **Chocolate**, **Facebook**, **Fluxloop**, **Fyber**, **Fysical**, **InMobi**, **Inner-Active**, **Ogury Presage**, **Safegraph**, **Receptiv**, **Unacast**, **Unity3d**, and **Vungle**. |
| Tinder | Sends GPS position and "target gender" to **AppsFlyer** and **LeanPlum**.<br>Sends Advertising ID to **AppsFlyer**, **Branch**, **Facebook**, and **Salesforce** (**Krux**). |
| Wave Keyboard | Sends Advertising ID to **Crashlytics**, **Facebook**, **Flurry**, **OneSignal**. |

*

Die meisten Apps senden teilweise sensible Daten an Drittparteien!

* Abb. aus "Out of Control" (Forbrukerrådet, 2020).

# Personalisierte Werbung



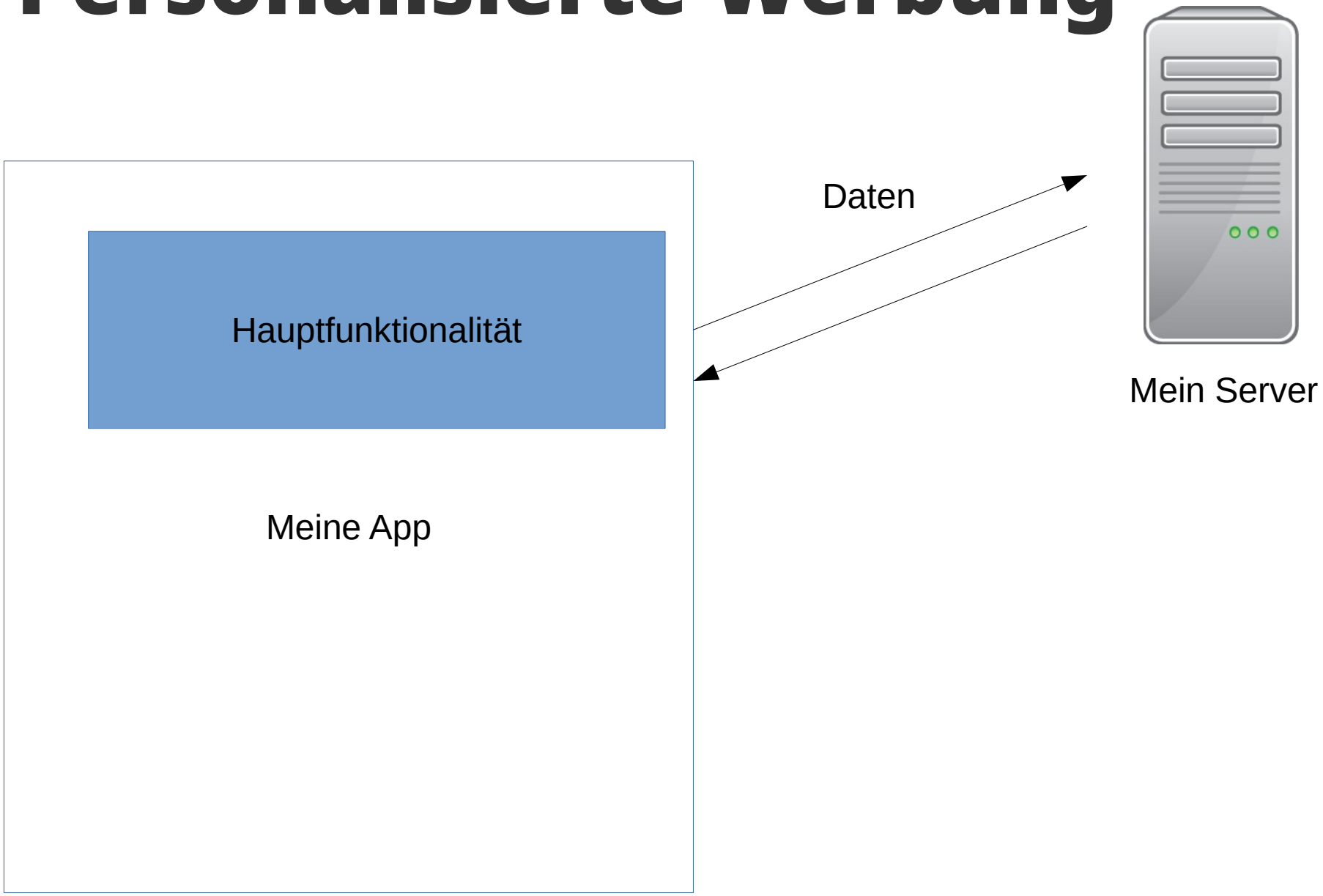
# Personalisierte Werbung

Mein Server

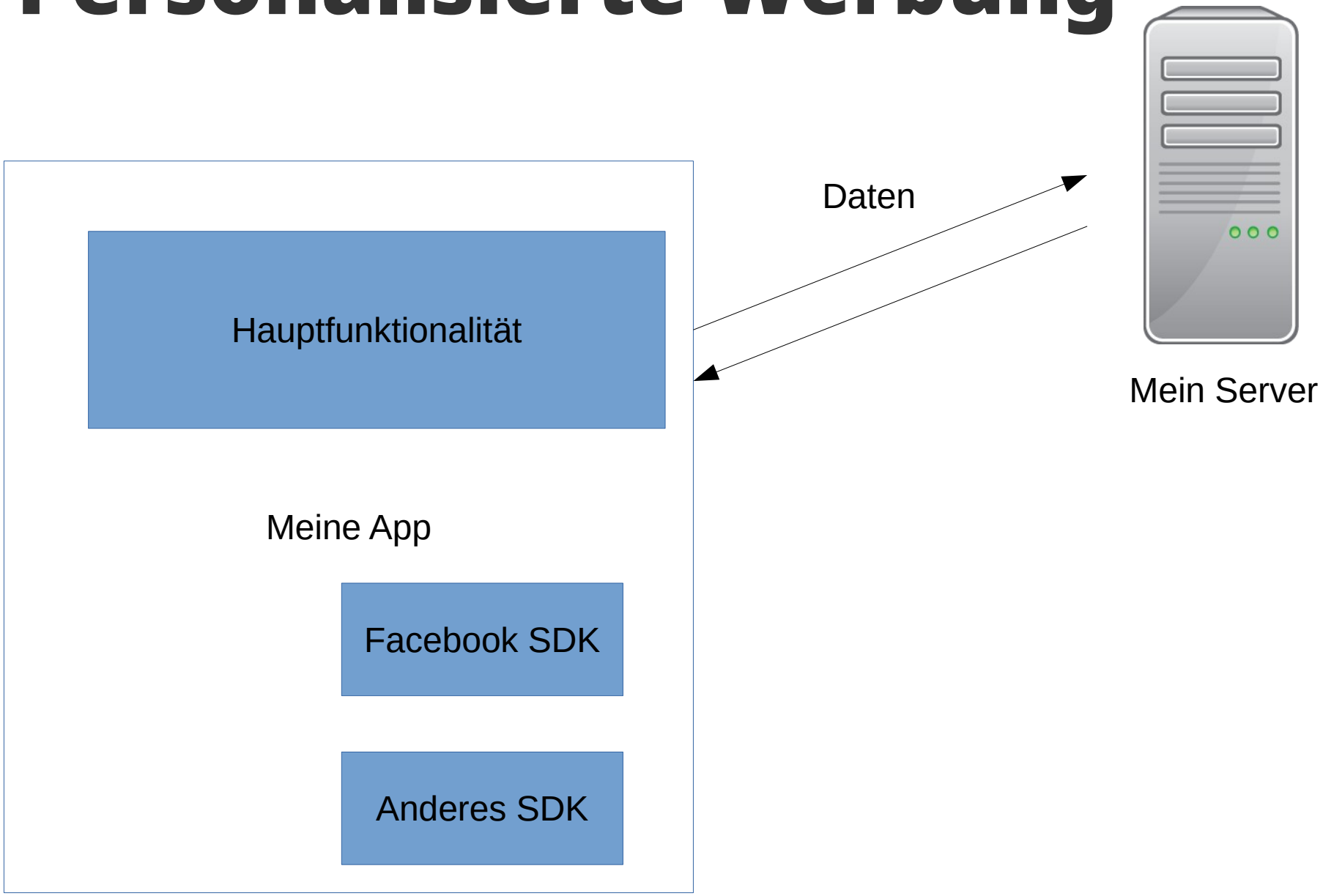
Hauptfunktionalität

Meine App

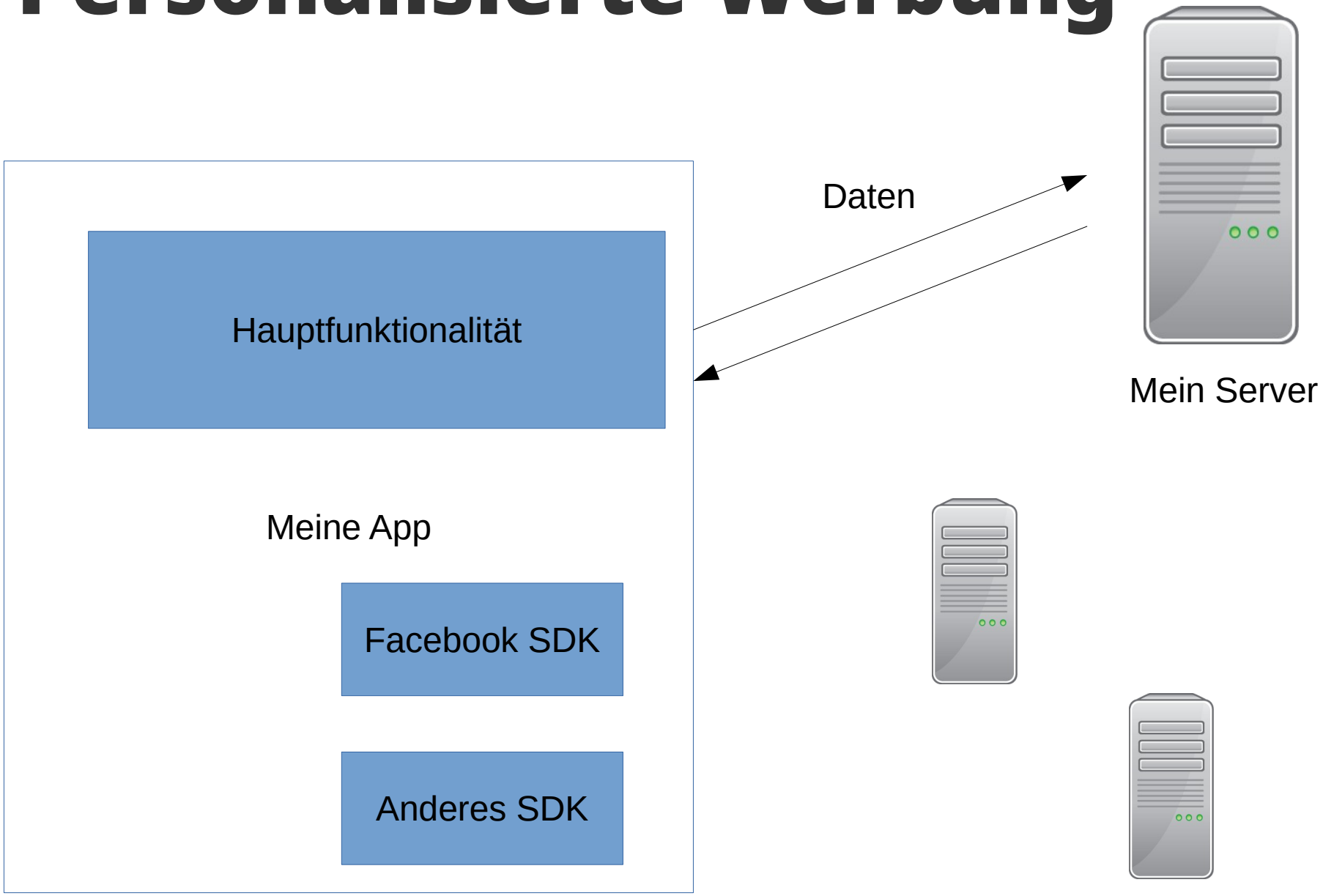
# Personalisierte Werbung



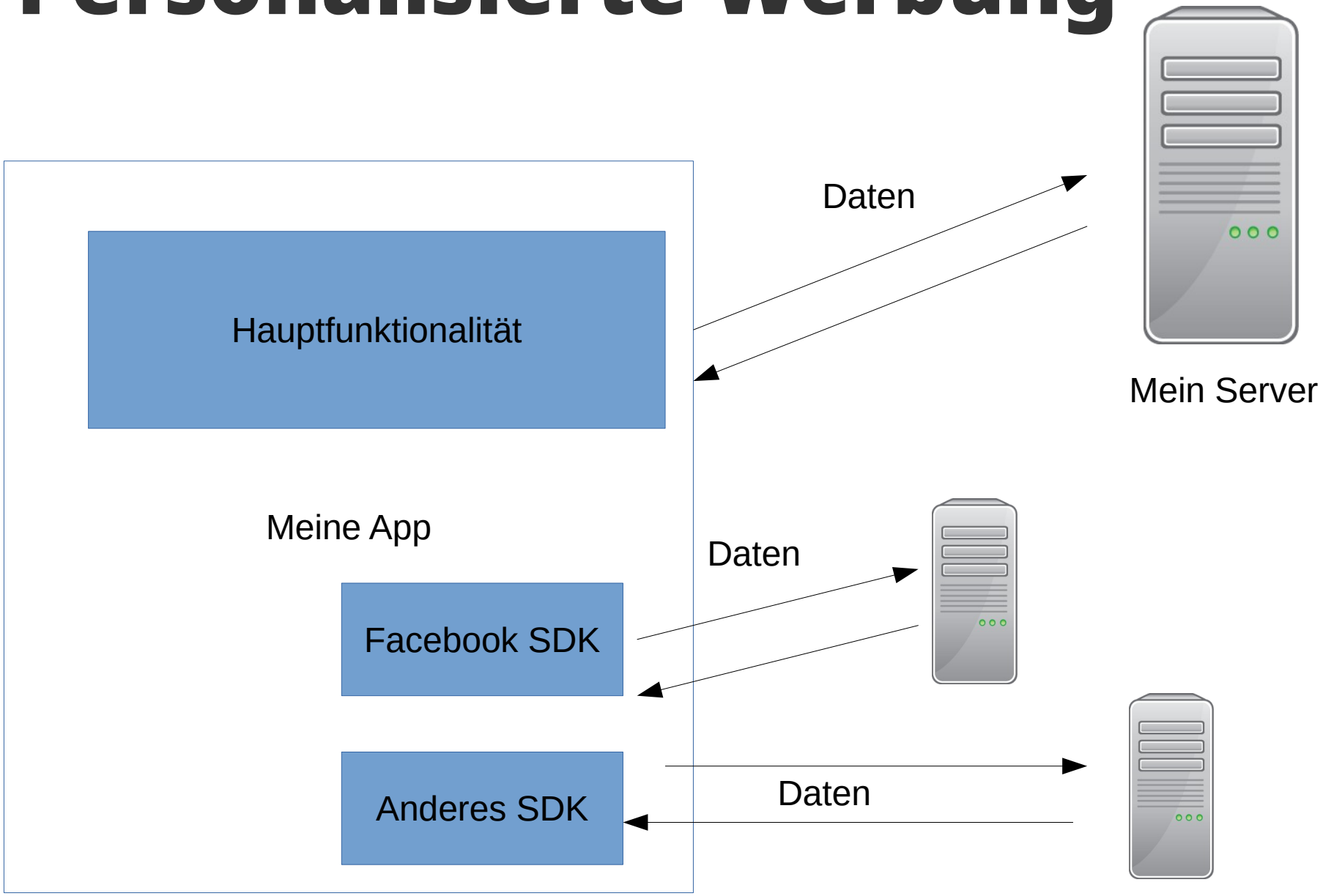
# Personalisierte Werbung



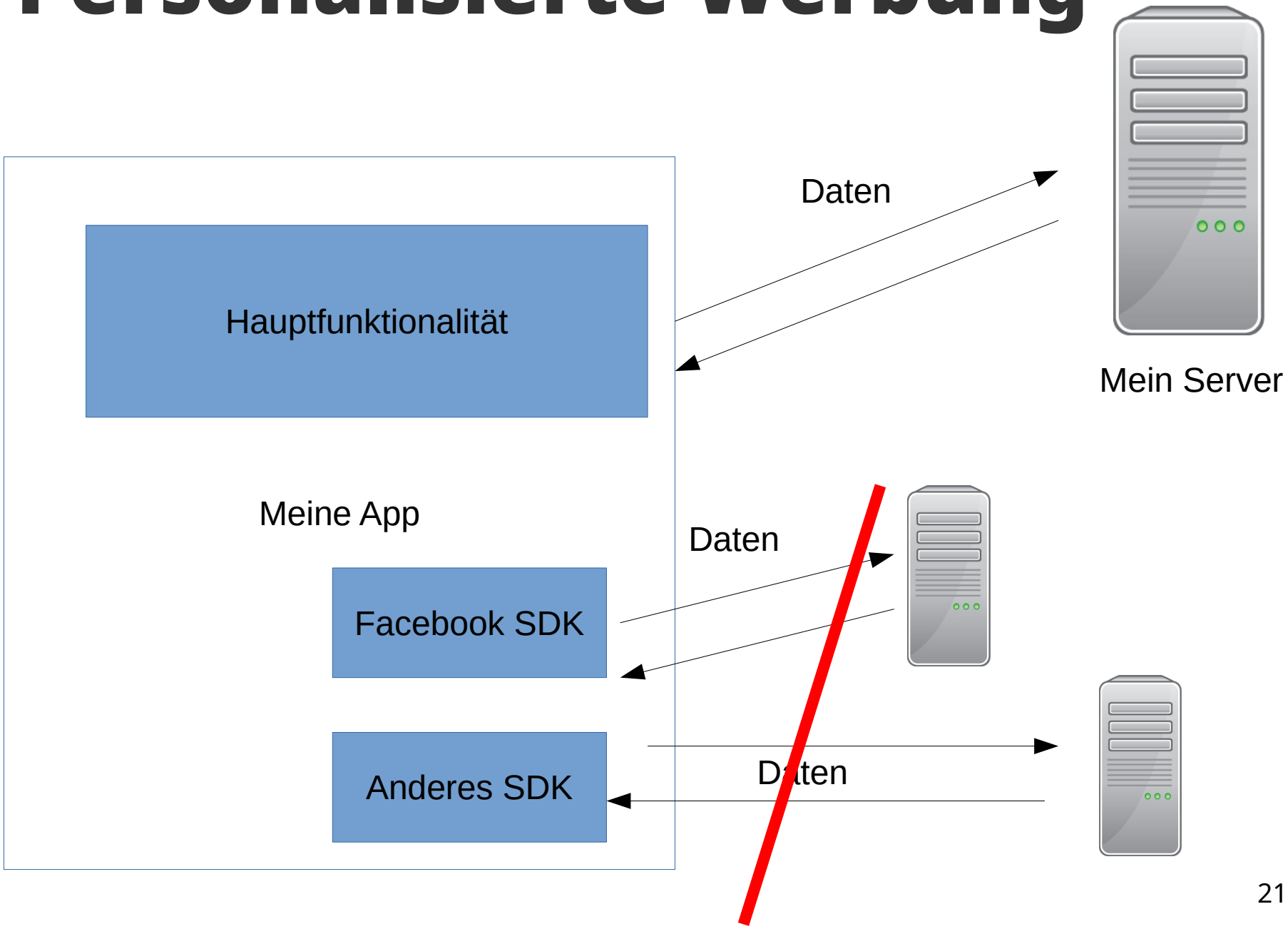
# Personalisierte Werbung



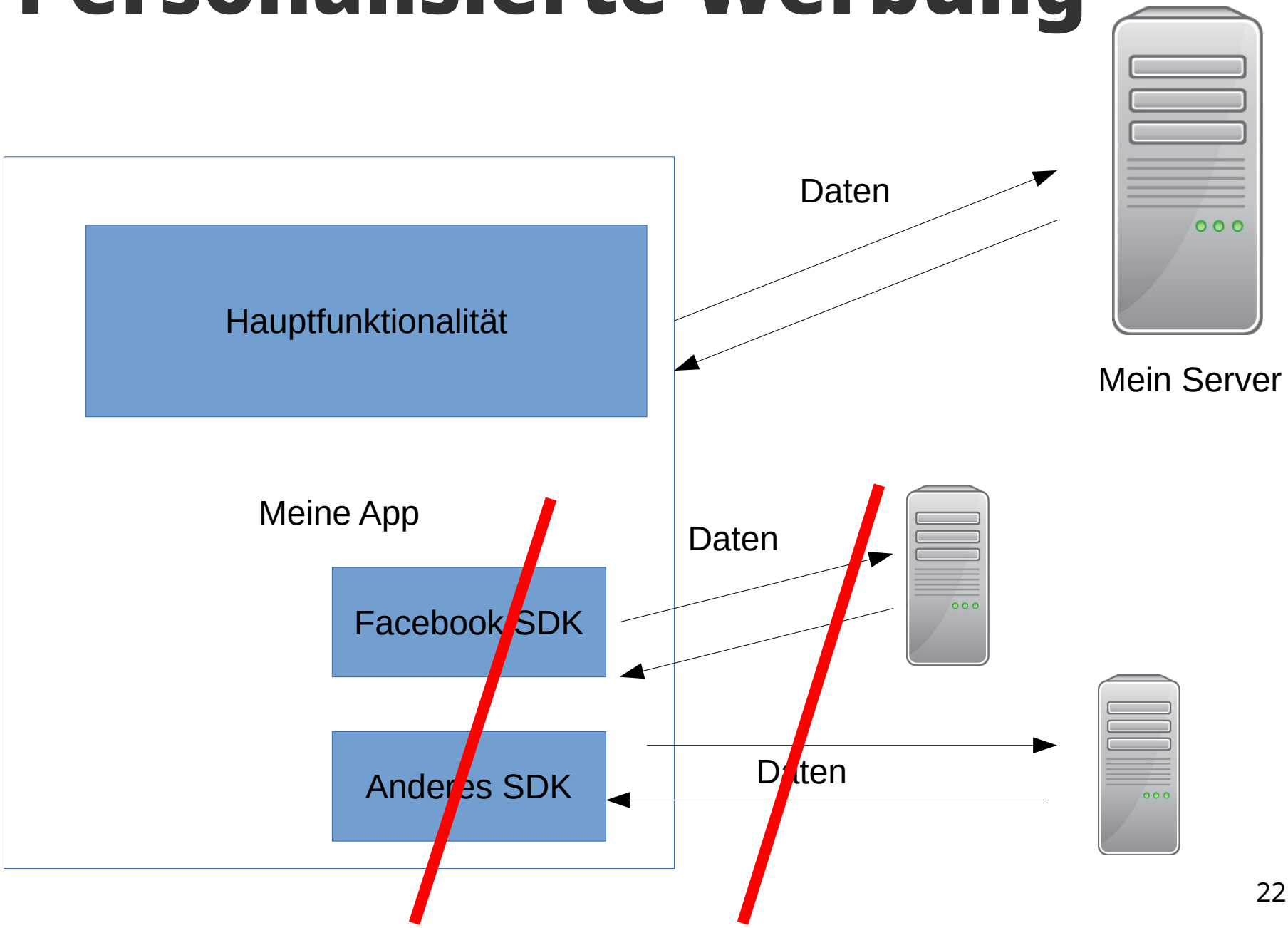
# Personalisierte Werbung



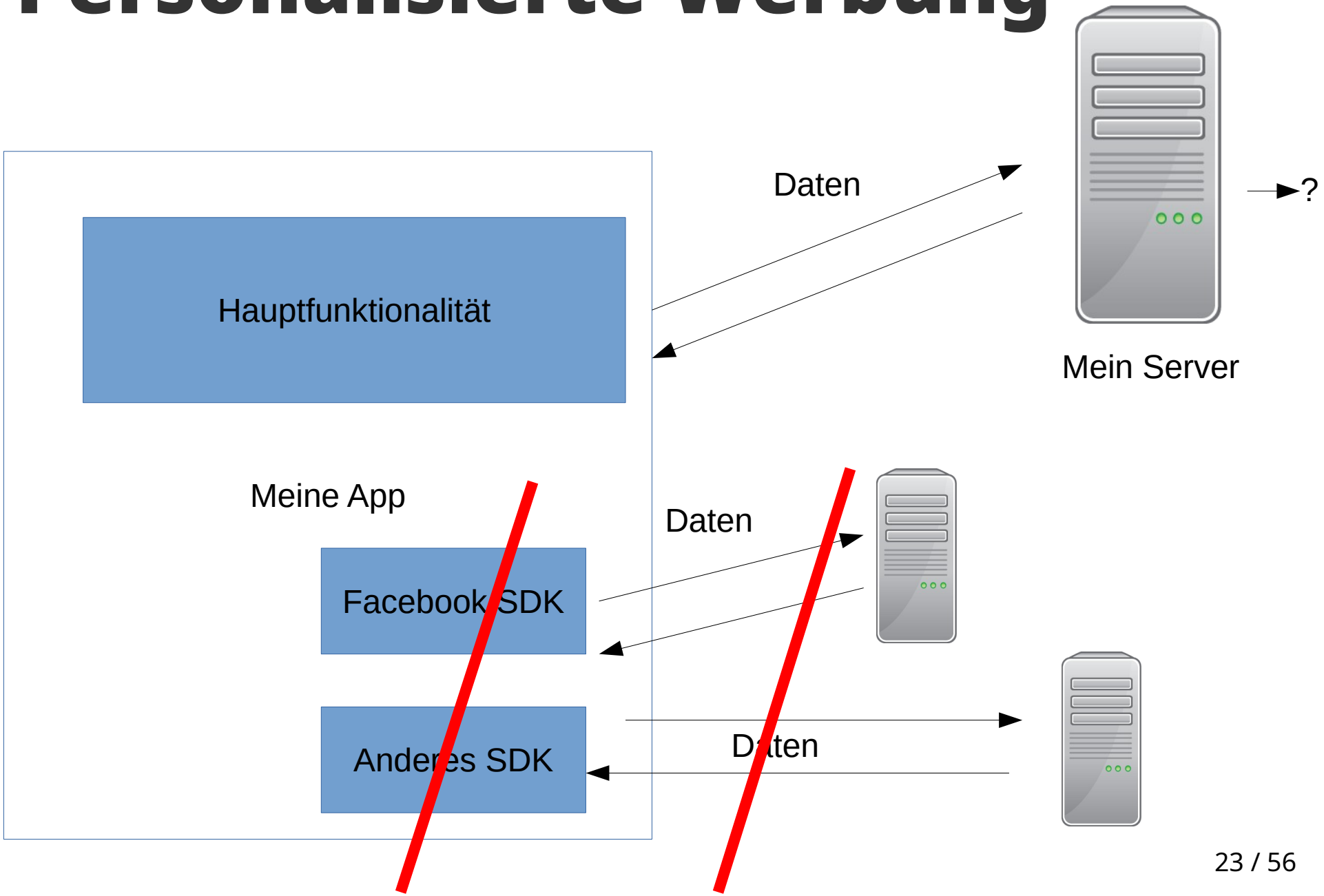
# Personalisierte Werbung



# Personalisierte Werbung



# Personalisierte Werbung



# Bonitätsbeurteilungen

- Beispiel: Schufa Holding AG
  - Daten kommen von Vertragspartnern (z.B. Bank bei der dein Konto liegt, Versandhandel)
  - Je höher Score, desto höher wird Kreditwürdigkeit eingeschätzt
  - Algorithmus nicht bekannt

# Bonitätsbeurteilungen

- Beispiel: Schufa Holding AG
  - Daten kommen von Vertragspartnern (z.B. Bank bei der dein Konto liegt, Versandhandel)
  - Je höher Score, desto höher wird Kreditwürdigkeit eingeschätzt
  - Algorithmus nicht bekannt
- Art. 15 Abs. 1 lit h DSGVO:
  - Offenlegung „aussagekräftige[r] Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ bei negativen Auswirkungen von automatisierten Einzelfallentscheidungen

# Bonitätsbeurteilungen

- Beispiel: Schufa Holding AG
  - Daten kommen von Vertragspartnern (z.B. Bank bei der dein Konto liegt, Versandhandel)
  - Je höher Score, desto höher wird Kreditwürdigkeit eingeschätzt
  - Algorithmus nicht bekannt
- Art. 15 Abs. 1 lit h DSGVO:
  - Offenlegung „aussagekräftige[r] Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ bei negativen Auswirkungen von automatisierten Einzelfallentscheidungen
  - keine automatisierte Einzelfallentscheidung im Sinne des Art. 22 Abs. 1 DSGVO *



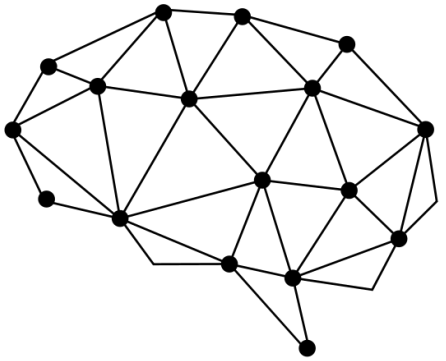
* “Die Schufa und ihre Intransparenz – ein Versagen der DSGVO?” - Datenschutzbeautragter-Info.de

# Bonitätsbeurteilungen

- Ergebnisse der OpenSchufa – Initiative
  - Probleme mit verschiedenen Versionen des Algorithmus
  - Ungenaue Daten
  - Teilweise negative Daten ohne ersichtlichen Grund
  - Schlechtere Scores für junge Männer

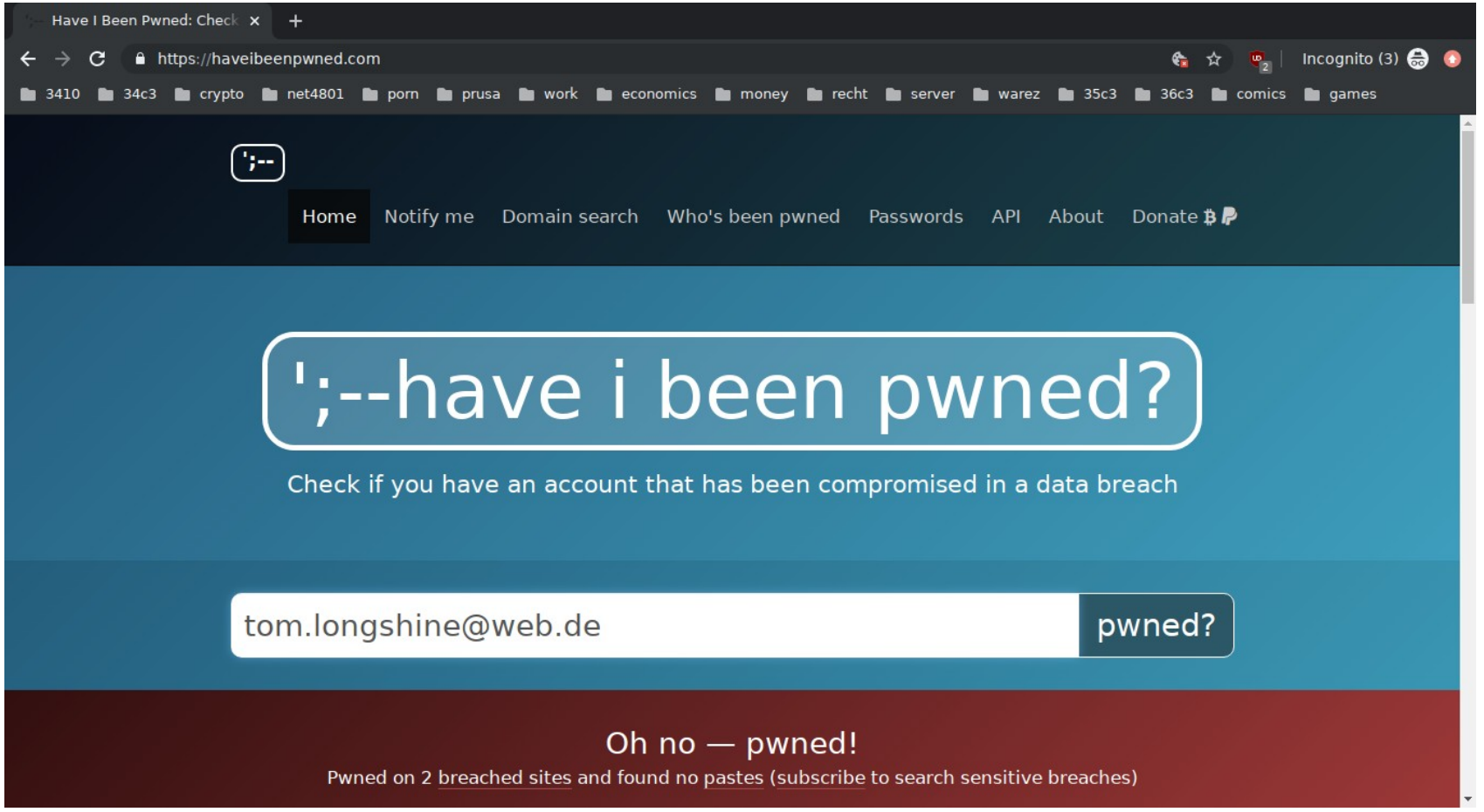
# Cambridge Analytica

- Individualisierte Werbung?
  $\rightarrow$ Individualisierter Wahlkampf!
- Involviert in die Trump- und Brexit-Wahlkampagnen
- Nutzt Daten u.a. von Facebook um gezielt Einfluss zu nehmen

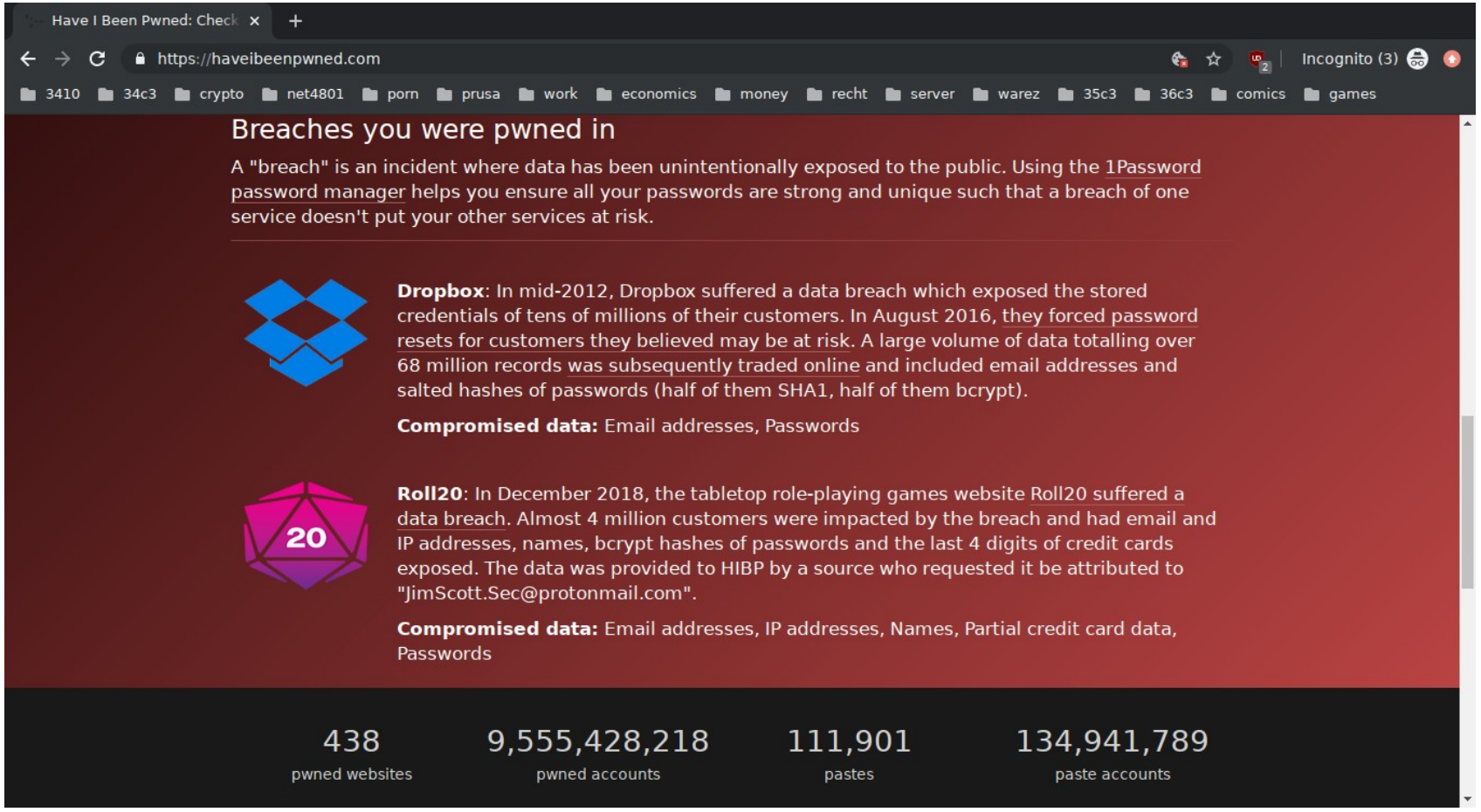


Cambridge Analytica

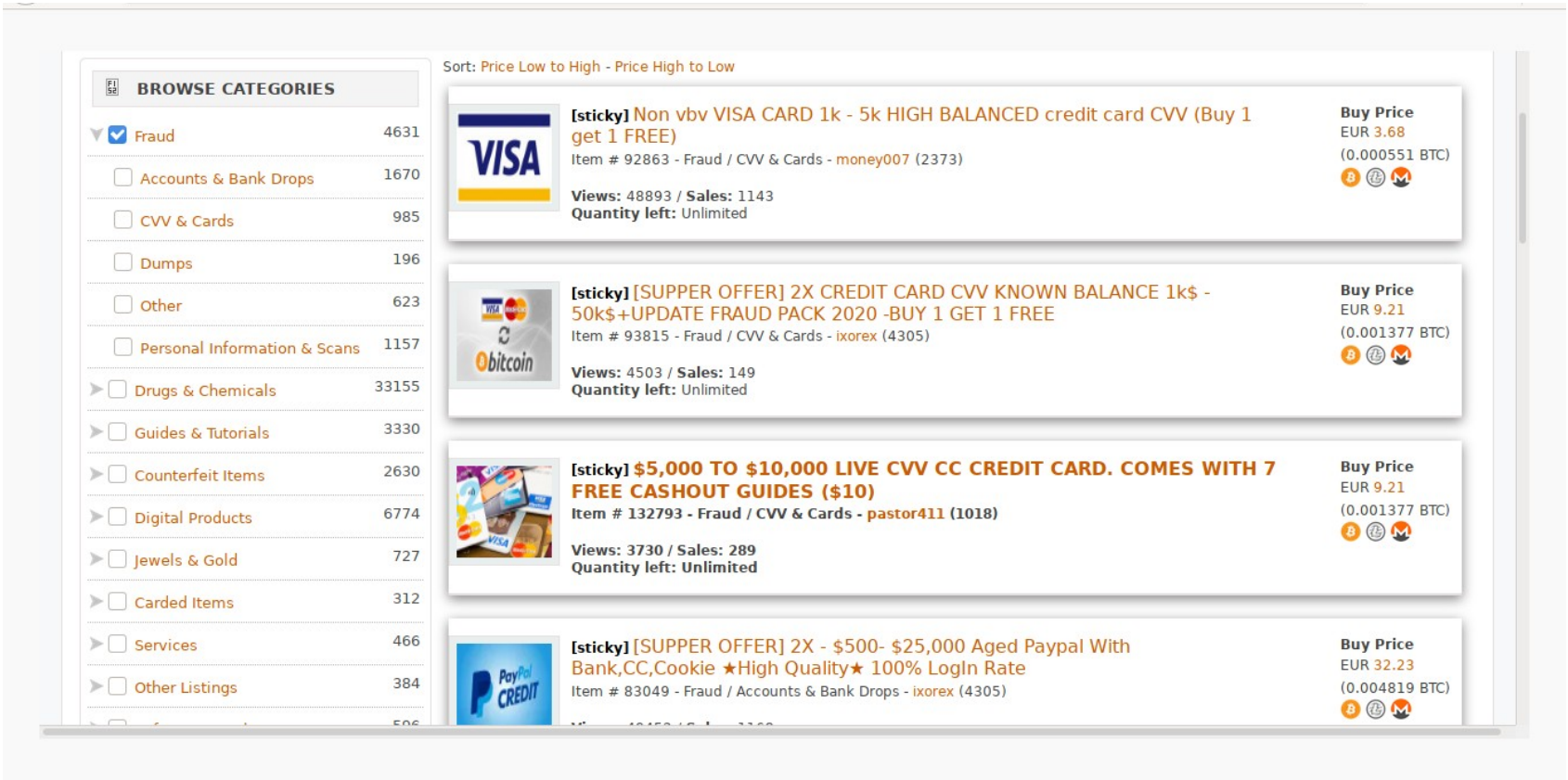
# “Datenreichtum” bei Unternehmen …



# “Datenreichtum” bei Unternehmen …



# … führt zu Reichtum bei Scammern



# Polizeidatenbanken

- Neben strafrechtlicher Historie auch
  - Politische Gesinnung
  - Drogen-Konsum
- Zunehmende Ermächtigung durch PAG
  - Überwachung und Präventivhaft für “Gefährder”

# Corona-App in China

- Einstufung in rote/gelbe/ grüne Risikoklasse
- Bewegungsfreiheit nur für grün
- Intransparente Funktionsweise
- Ähnliche Überlegungen auch in Deutschland

# Fazit vor der Pause

- Schutz personenbezogener Daten → Schutz der Freiheit und Unversehrtheit einer Person

# Fazit vor der Pause

- Schutz personenbezogener Daten → Schutz der Freiheit und Unversehrtheit einer Person
- Unternehmen, Staaten, Wissenschaft, etc haben andere Interessen/Gründe um an unsere Daten zu kommen

# Fazit vor der Pause

- Schutz personenbezogener Daten → Schutz der Freiheit und Unversehrtheit einer Person
- Unternehmen, Staaten, Wissenschaft, etc haben andere Interessen/Gründe um an unsere Daten zu kommen
- Eine Person die deine Daten besitzt kann sie immer gegen dich verwenden

# Fazit vor der Pause

- Schutz personenbezogener Daten → Schutz der Freiheit und Unversehrtheit einer Person
- Unternehmen, Staaten, Wissenschaft, etc haben andere Interessen/Gründe um an unsere Daten zu kommen
- Eine Person die deine Daten besitzt kann sie immer gegen dich verwenden

**Nach der Pause: Datenschutz umsetzen**

# Pause?

# Wie schützen?

- Allgemeines Problem:
  - Interessensgruppen mit unterschiedlichen Ressourcen
- Hilfreiche Forderungen:
  - Prinzip der Datensparsamkeit
  - Transparenz
  - Sicherheitsmechanismen
  - Dezentrale Infrastruktur
- Beispiele: Individuelle Schutzmaßnahmen
- Technologie vs. Politik

# Prinzip der Datensparsamkeit

- Als Forderung an die Gesellschaft (Unternehmen, Politik, andere Organisationen):
  - Erforderlichkeit: nur Daten holen, verarbeiten, weitergeben wenn es wirklich erforderlich ist
  - Zweckbindung: diese Daten nur für den ursprünglichen Zweck verwenden
- Als persönliche Umsetzung:
  - Datenspuren minimieren (Pseudonyme verwenden, Kontaktbücher nicht syncen, Leute nicht ohne Erlaubnis taggen etc.)

# Transparenz

- Als Forderung an die Gesellschaft:
  - Code und Algorithmen veröffentlichen
  - Information der Betroffenen Person über Nutzung und Speicherung der Daten
- Als persönliche Umsetzung:
  - DSGVO-Anfragen nutzen: https://www.datenanfragen.de/
  - Andere Anfragearten nutzen: https://www.datenschmutz.de/moin
  - Quelloffene Software bevorzugen

# Sicherheitsmechanismen

- Als Forderung an die Gesellschaft:
  - Vertraulichkeit + Integrität mit aktuellen Technologien sicherstellen
    - z.B. aktuelle Verschlüsselungs und Signaturtechnologie breitflächig anwenden
    - z.B. Bugs fixen
- Als persönliche Umsetzung:
  - Updates installieren und aktuelle Software verwenden
  - Guidelines für sicheren Umgang im Internet beachten

# Dezentrale Infrastruktur

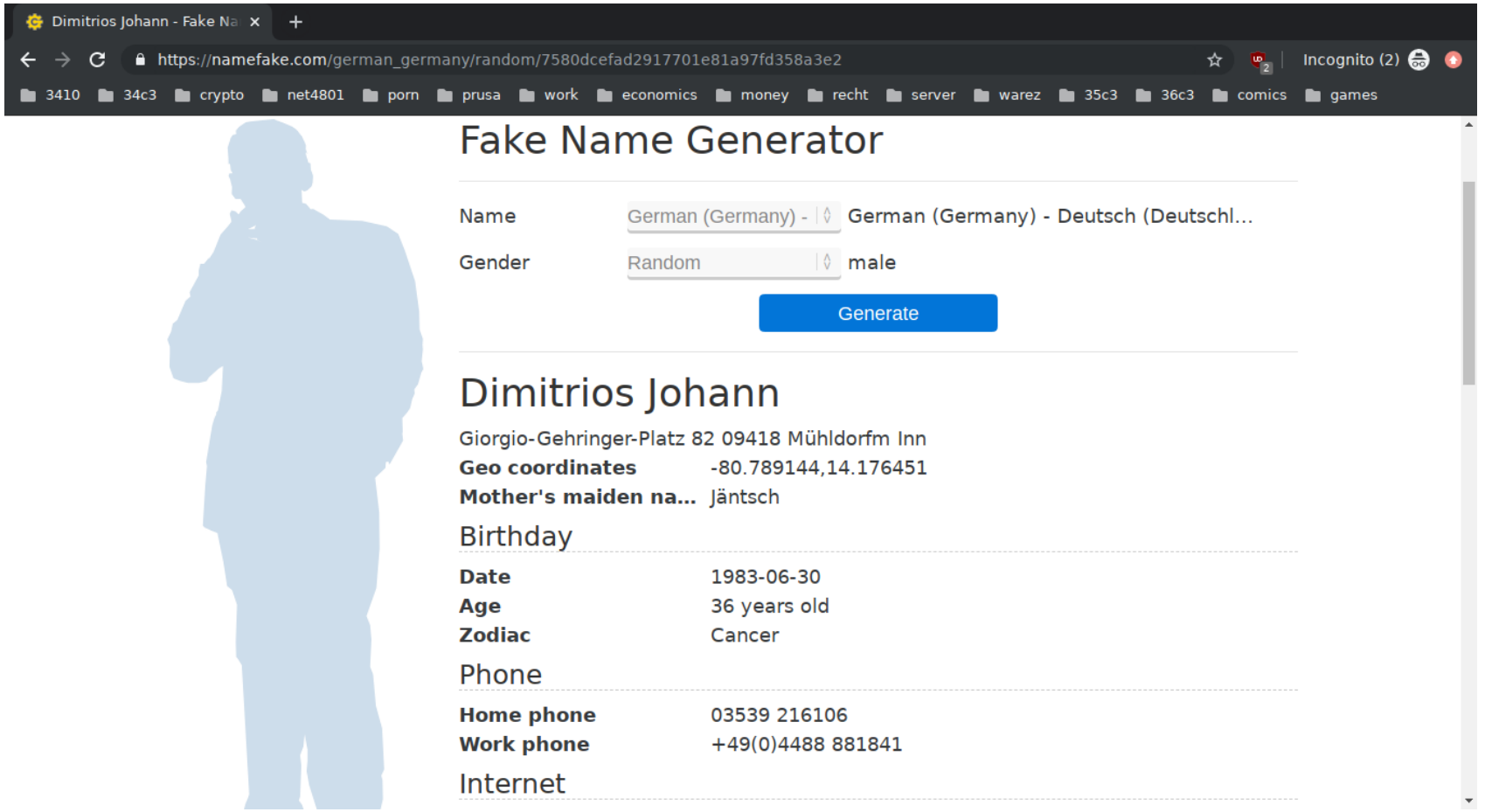
- Als Forderung an die Gesellschaft:
  - Zentralisierte Anhäufungen von Daten vermeiden
- Als persönliche Umsetzung:
  - Email bei riseup/systemli/... statt gmail/hotmail/...
  - Jabber statt WhatsApp
  - Mastodon statt Twitter
  - Diaspora statt Facebook
  - Peertube statt Youtube
  - Pixelfed statt Instagram

# Individueller Schutz

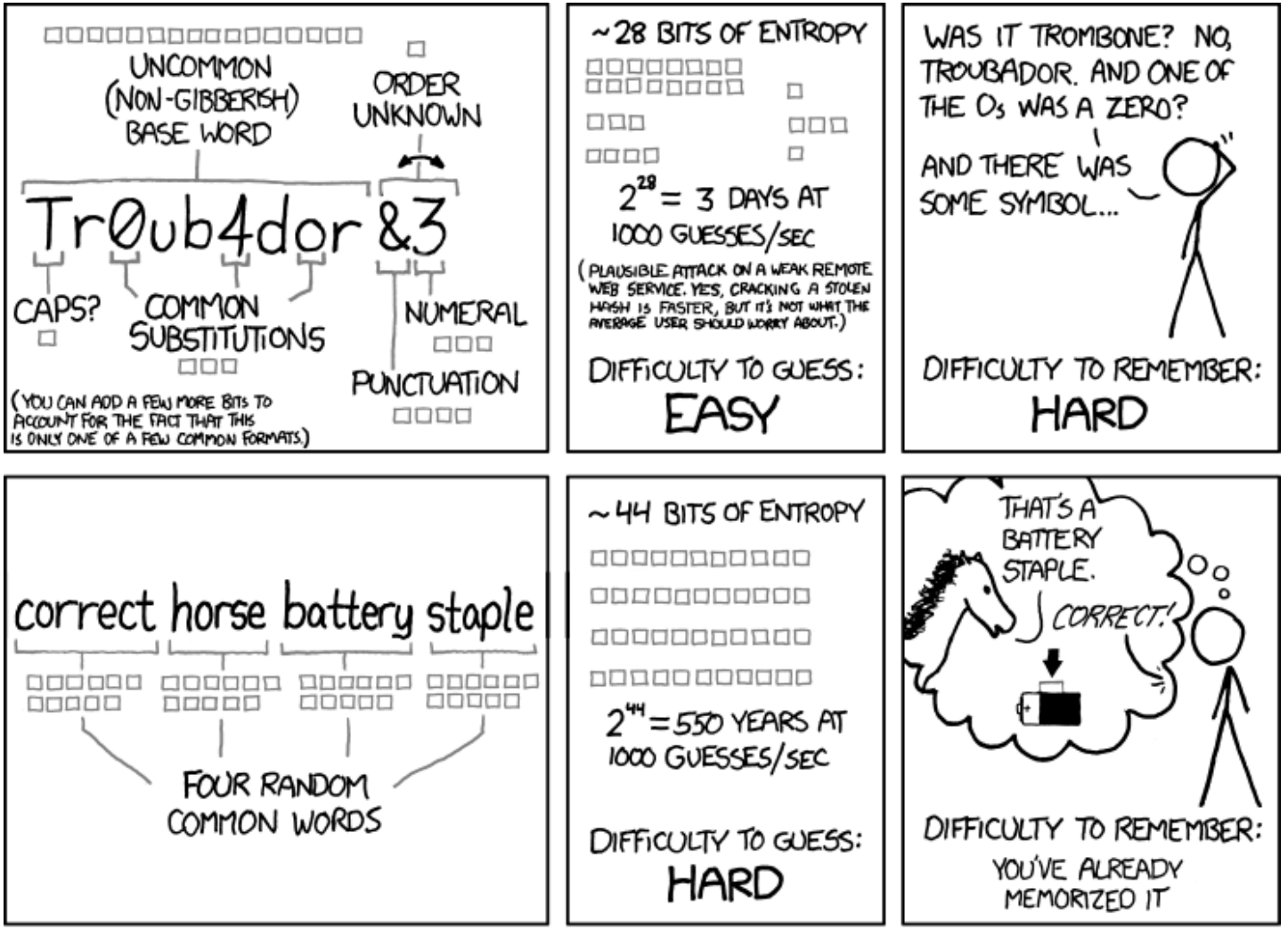
Grundregeln:

- Nicht auf jeden scheiß klicken und nicht überall personenbezogene Daten eingeben
- Sichere Passwörter wählen
- Updates installieren
- AdBlocker und Incognito Mode verwenden
- Verschlüsselung verwenden
- Offene, dezentrale Software verwenden

# Fake-Name-Generator



# Passwörter


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

# … aber das kann ich mir doch gar nicht merken

- Nutzt Passwortmanager!
  - Keepass2
  - bitwarden
- Ein starkes Masterpasswort
- Zufällig generierte Passwörter pro Seite

# Software-Update FAQ

- Muss ich wirklich?
  - Ja.

# Software-Update FAQ

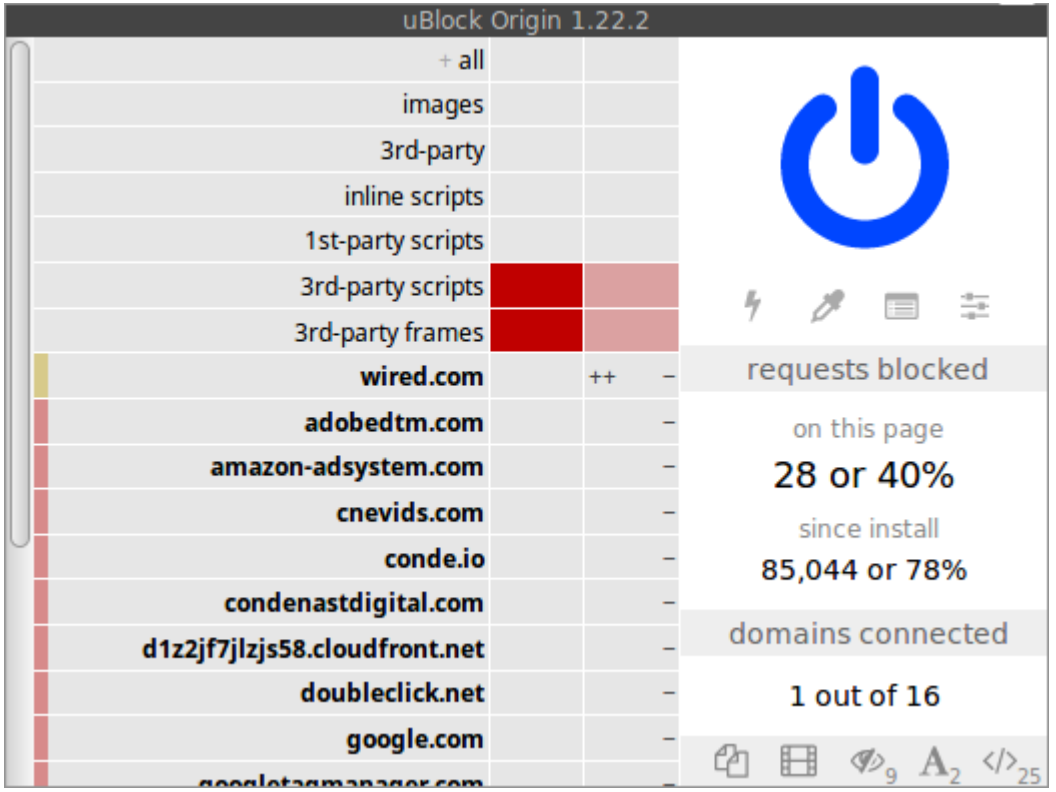
- Muss ich wirklich?
  - Ja.
- Kann es sein, dass dadurch Dinge kaputt gehen?
  - Sollte nicht, aber leider nicht komplett auszuschließen :(

# Software-Update FAQ

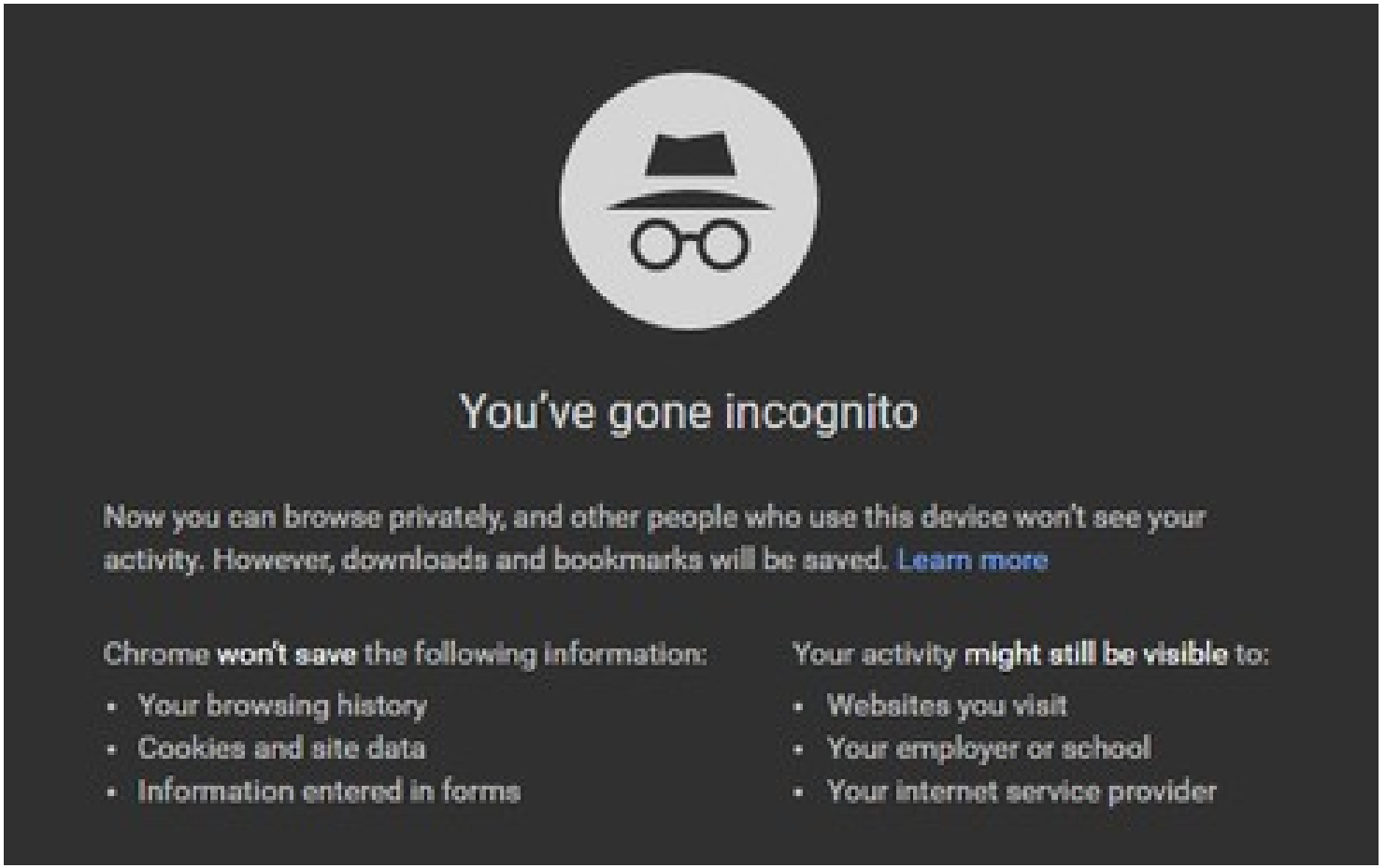
- Muss ich wirklich?
  - Ja.
- Kann es sein, dass dadurch Dinge kaputt gehen?
  - Sollte nicht, aber leider nicht komplett auszuschließen :(
- Muss ich trotzdem?
  - Ja.

# uBlock Origin

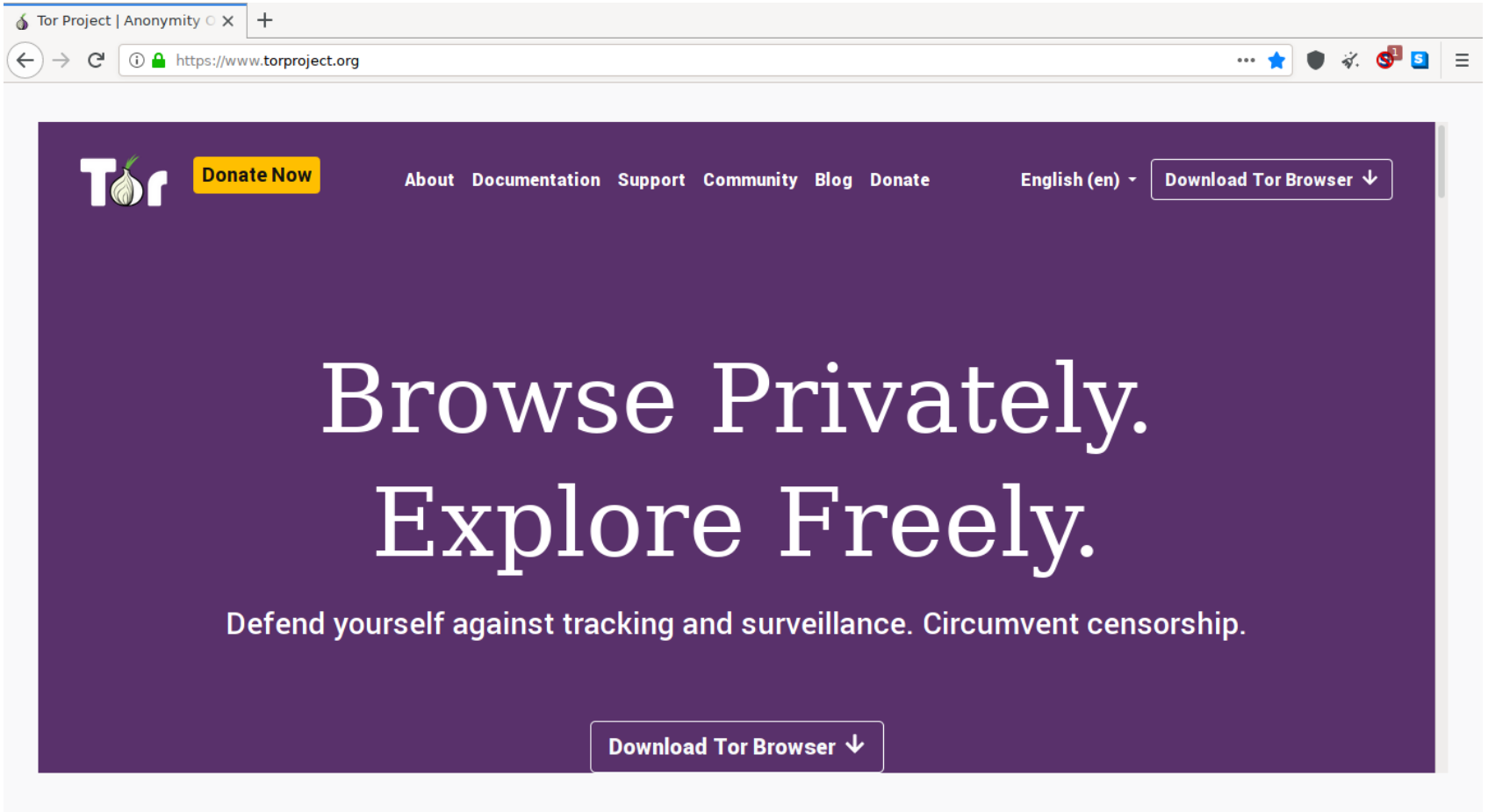
- Blocker für Ad- & Trackingnetzwerke und bekannte Malwaresites
- Verfügbar für die meisten Browser



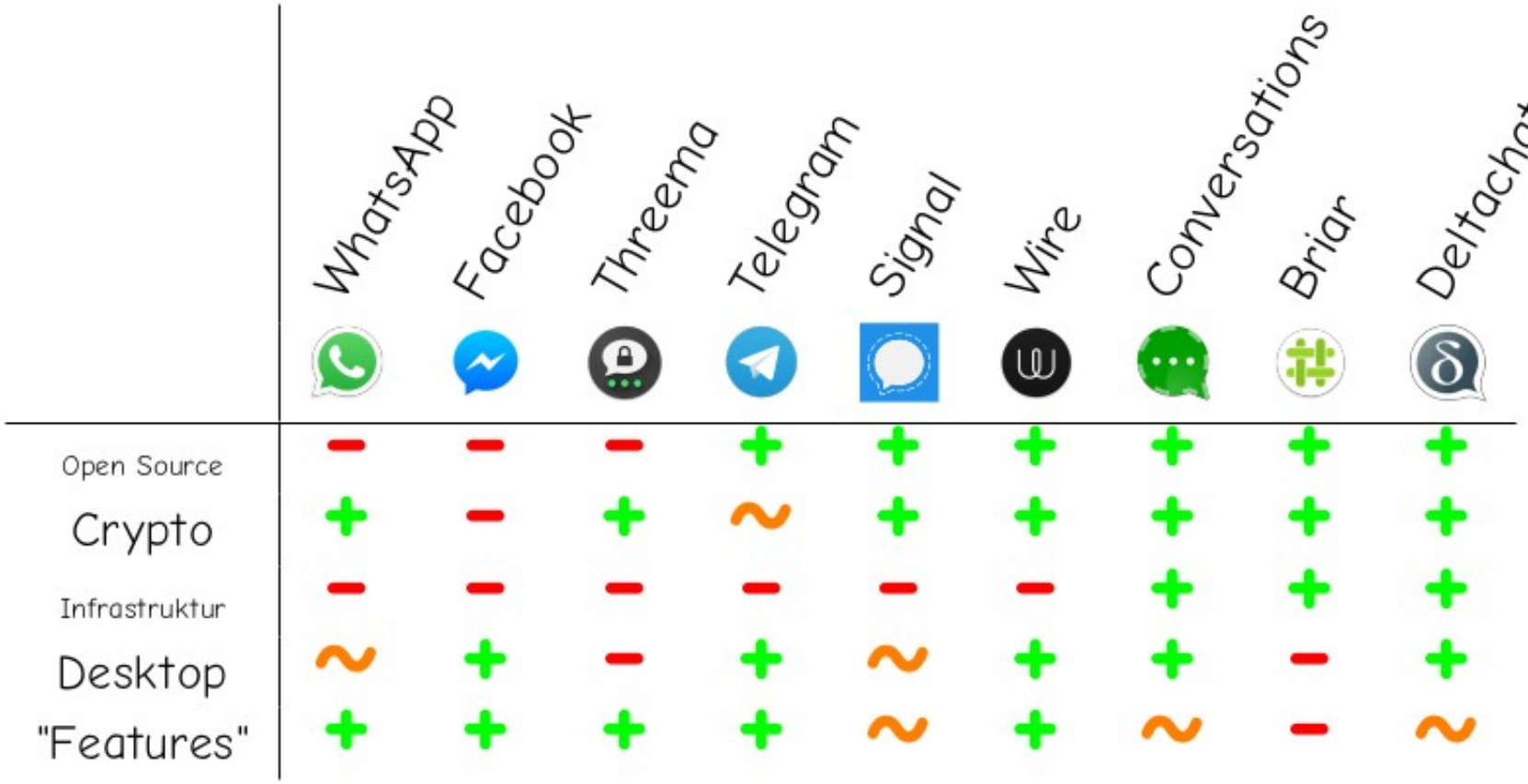
# Incognito Mode



# Tor Browser

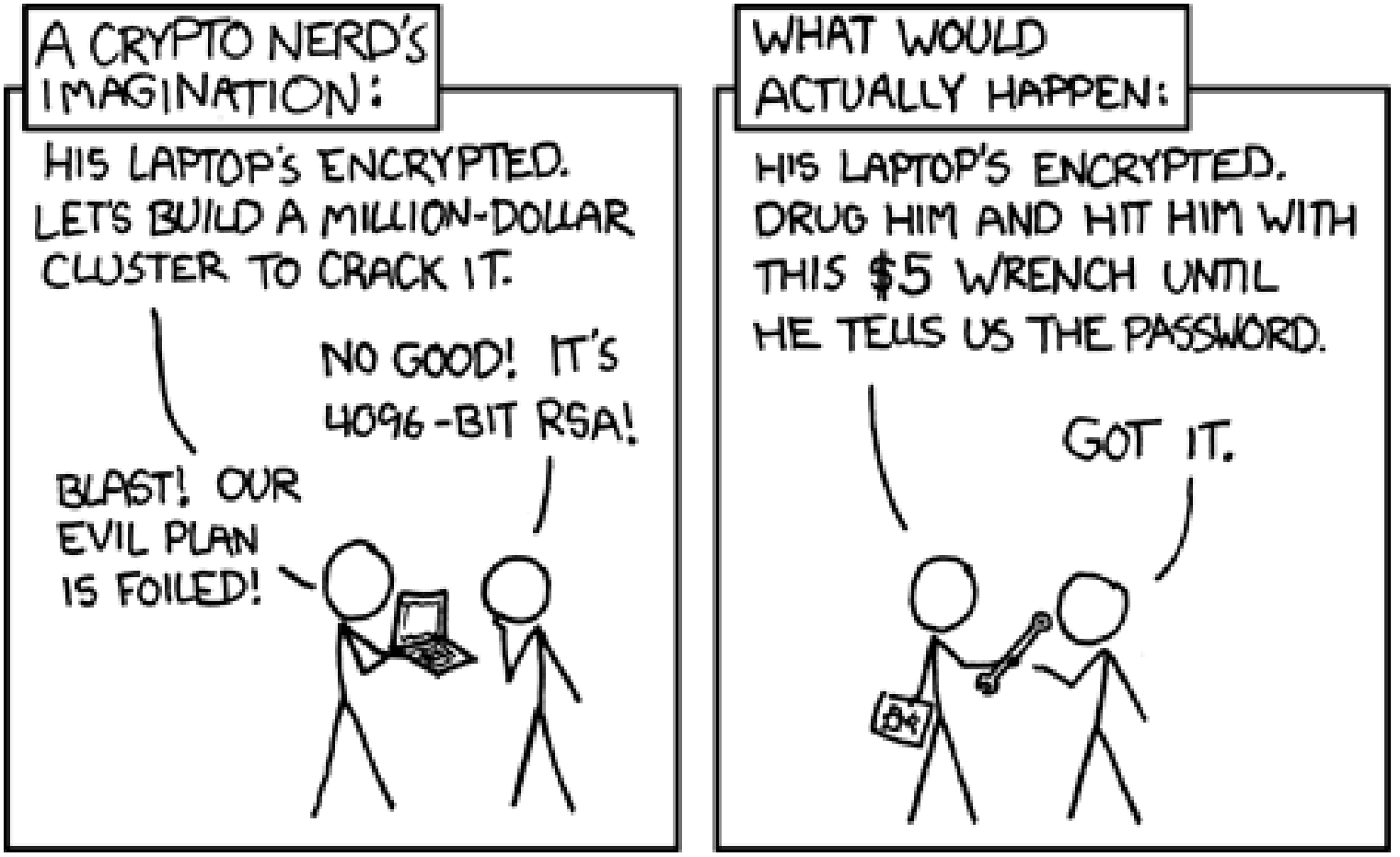

Tor Project | Anonymity
https://www.torproject.org
Donate Now
About
Documentation
Support
Community
Blog
Donate
English (en)
Download Tor Browser
Browse Privately.
Explore Freely.
Defend yourself against tracking and surveillance. Circumvent censorship.
Download Tor Browser

# Verschlüsselung




Weiter Infos: https://www.securemessagingapps.com

# Technologie vs. Politik



# Fazit

- Datensparsamkeit schützt vor Übergriffen durch Unternehmen/Scammern/Staaten
  → Bleibt anonym!
- Transparenz/Löschanfragen als Mittel sich zu entziehen → Nutzt die DSGVO!
- Dezentralisierung macht Übergriffe schwerer → Nutzt freie Software!
- Technologie kann politische Forderungen nicht ersetzen → Bleibt aktiv!