



# **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

0x90.space

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

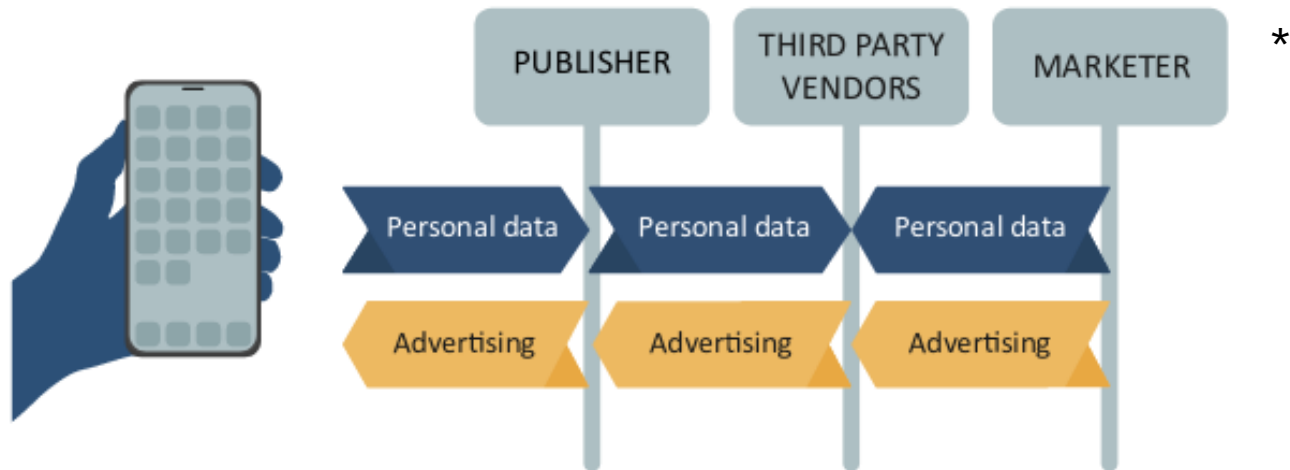
**Personenbezogene Daten zu besitzen  
bedeutet eine gewisse Macht zu besitzen.**



# 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

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

\*

Die meisten Apps senden teilweise sensible Daten an Drittparteien!

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

# Personalisierte Werbung

Meine App

# Personalisierte Werbung



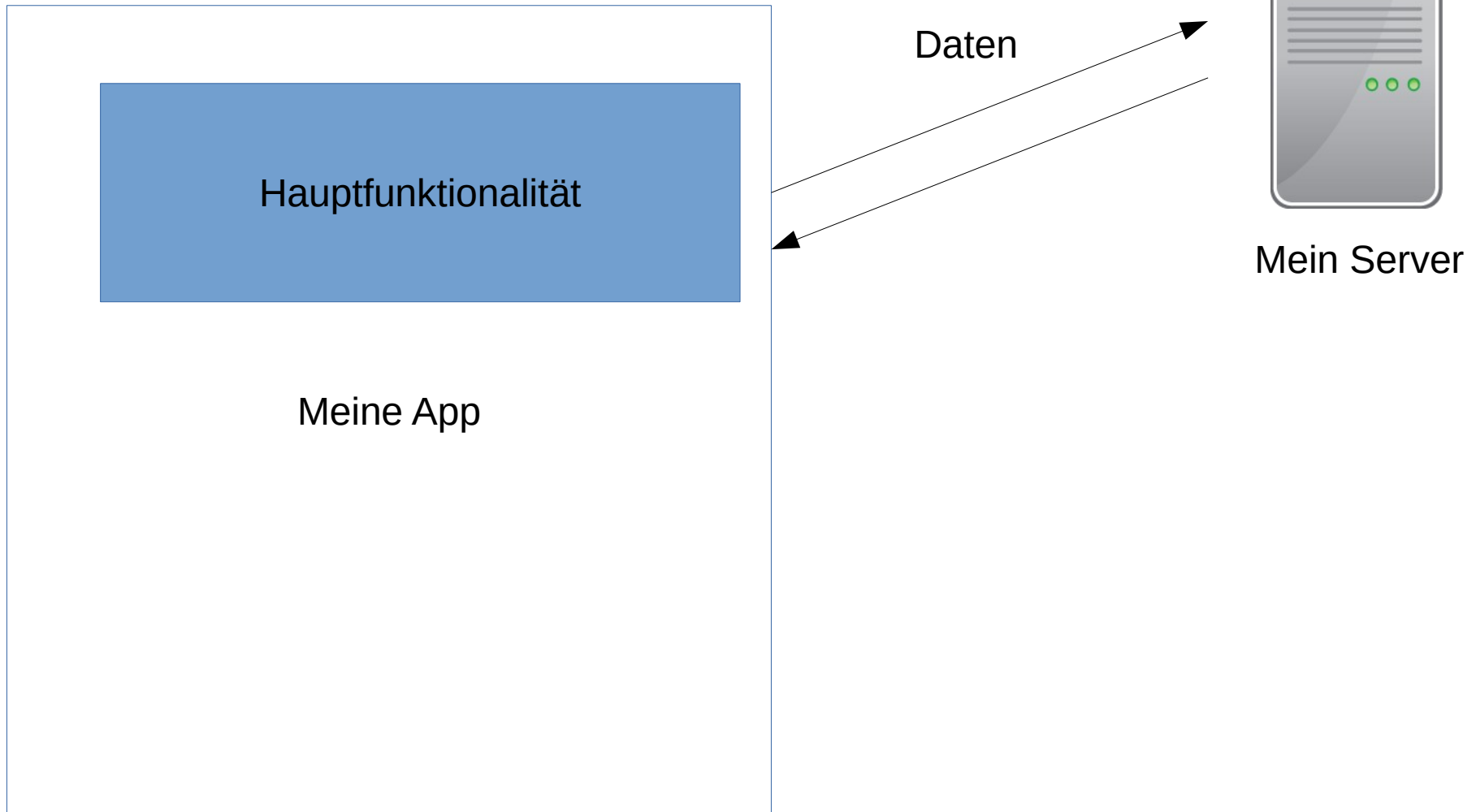
Mein Server

Hauptfunktionalität

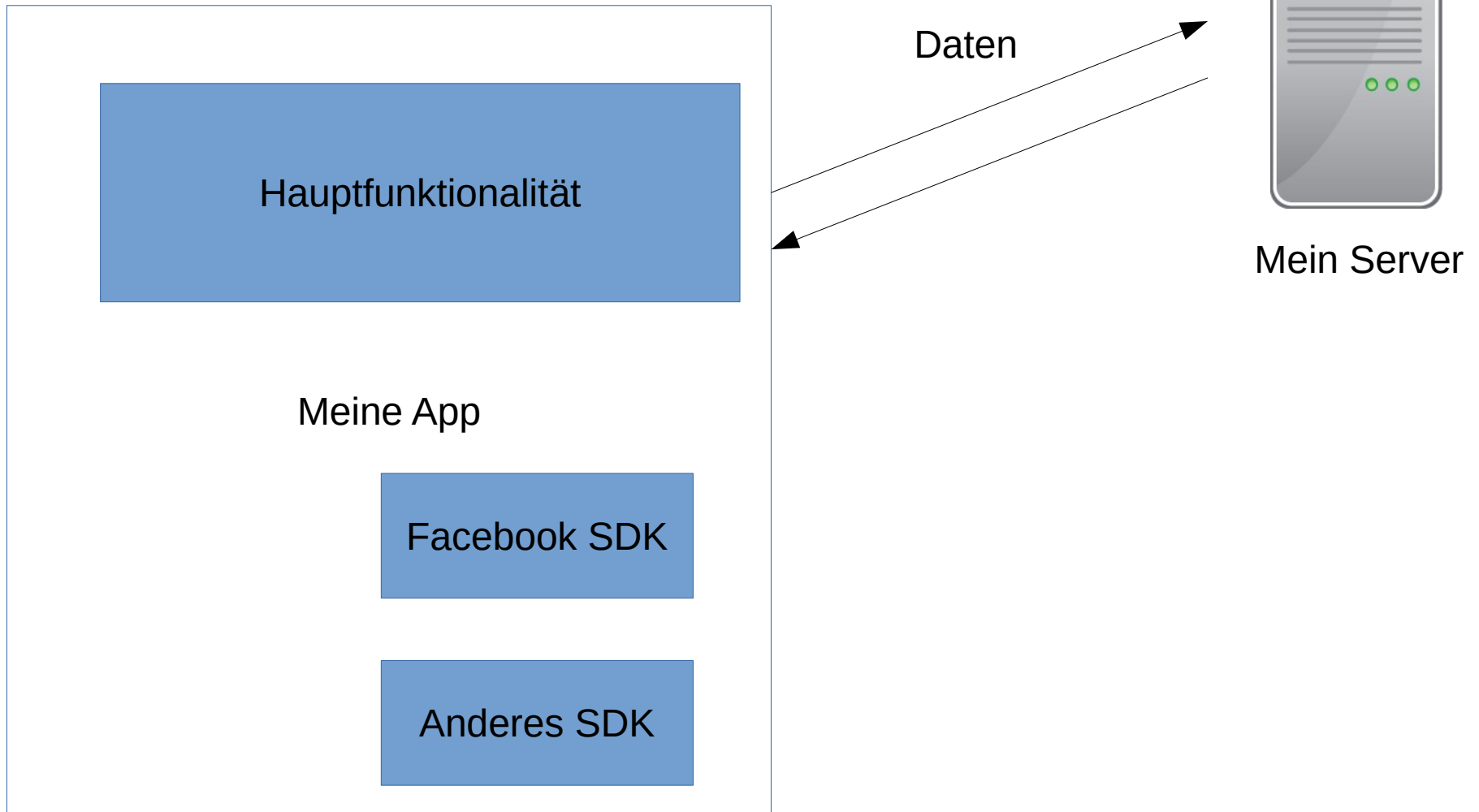
Meine App



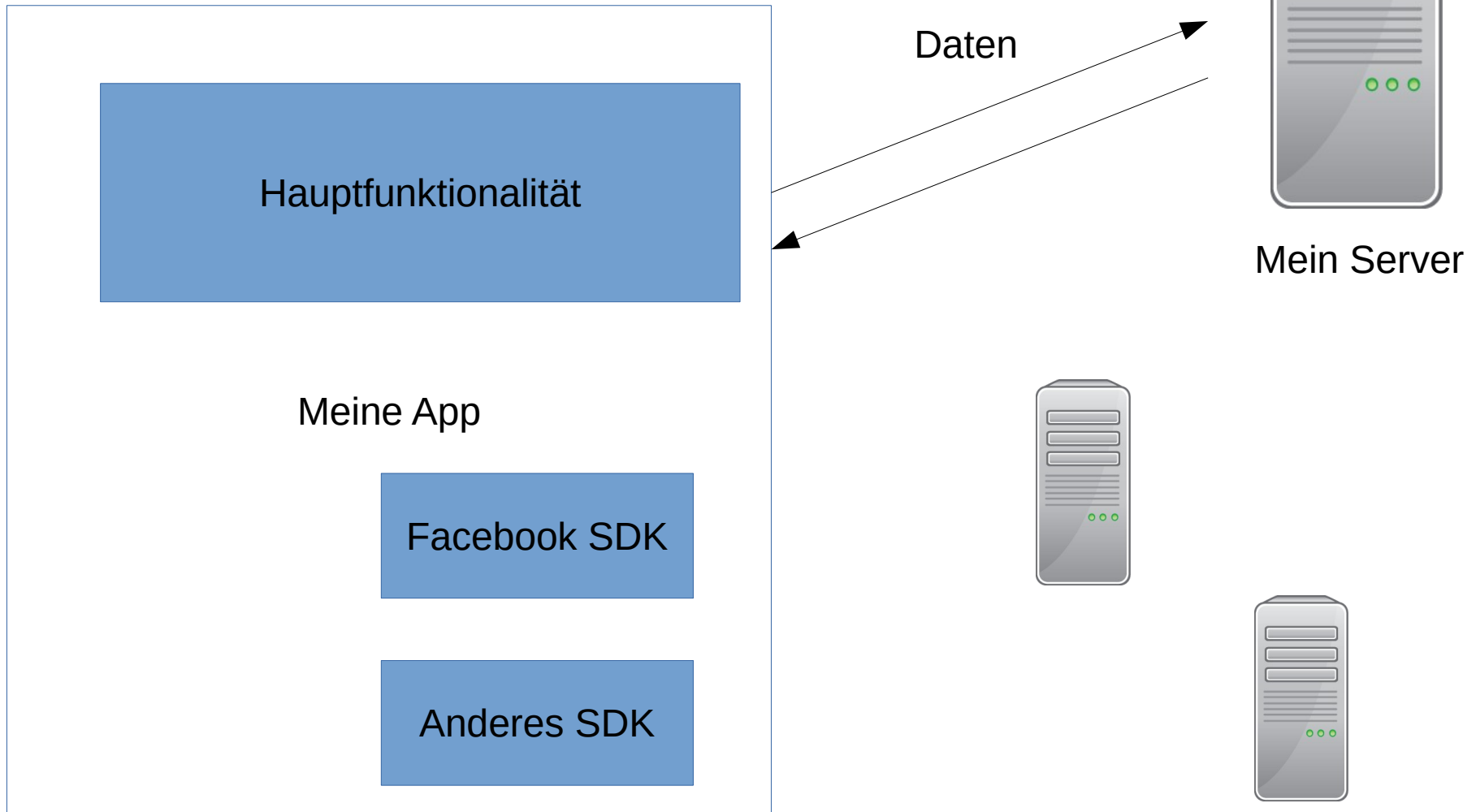
# Personalisierte Werbung



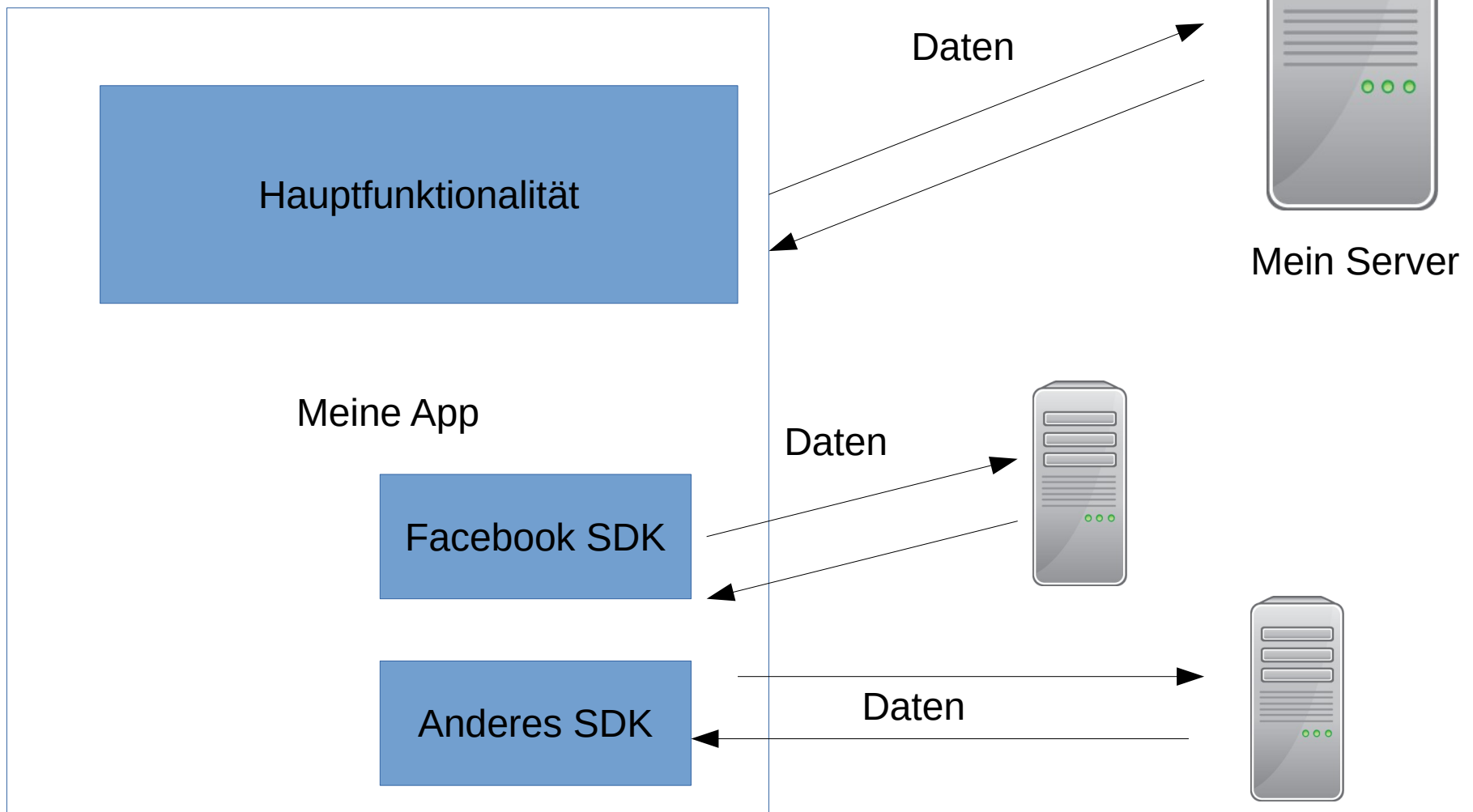
# Personalisierte Werbung



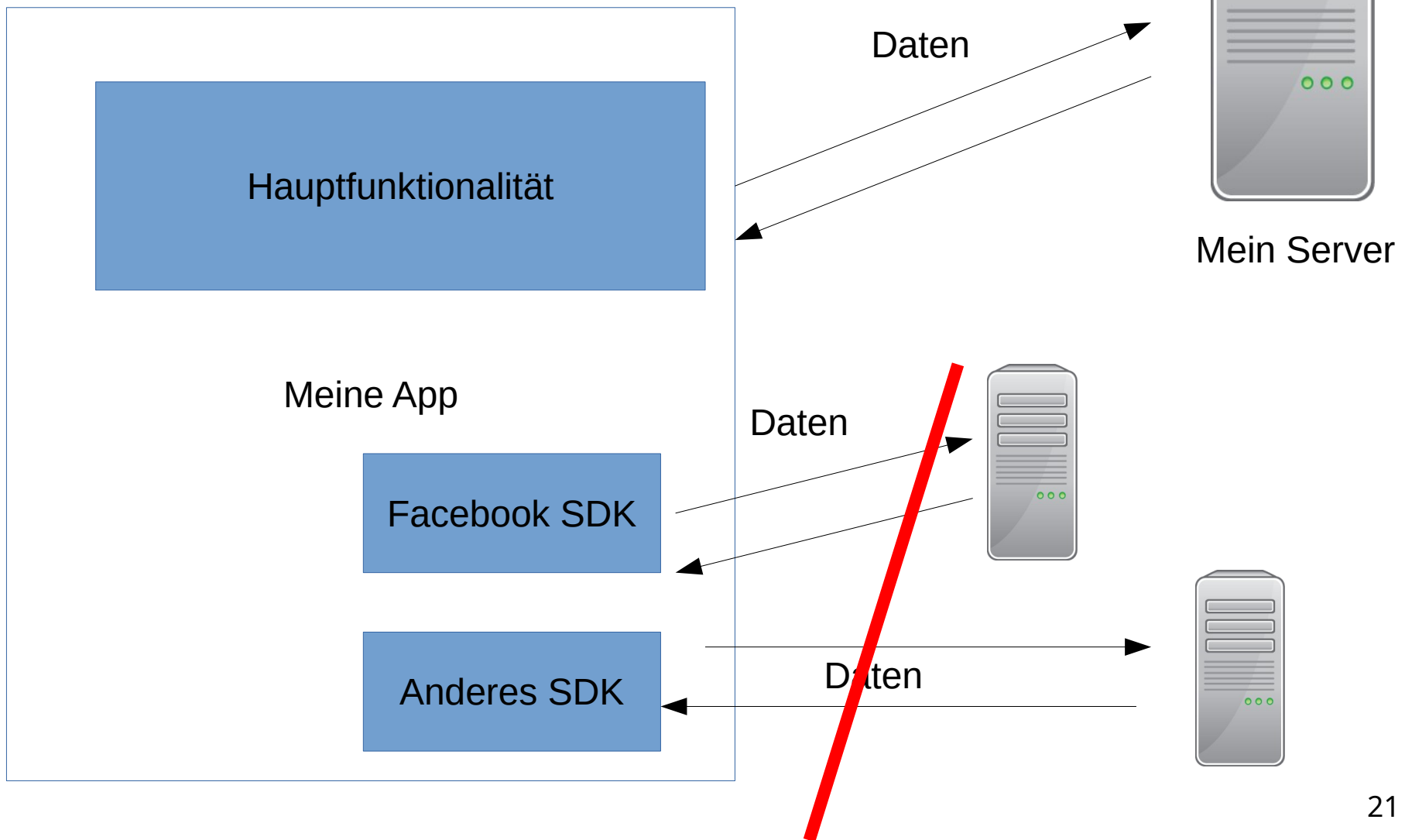
# Personalisierte Werbung



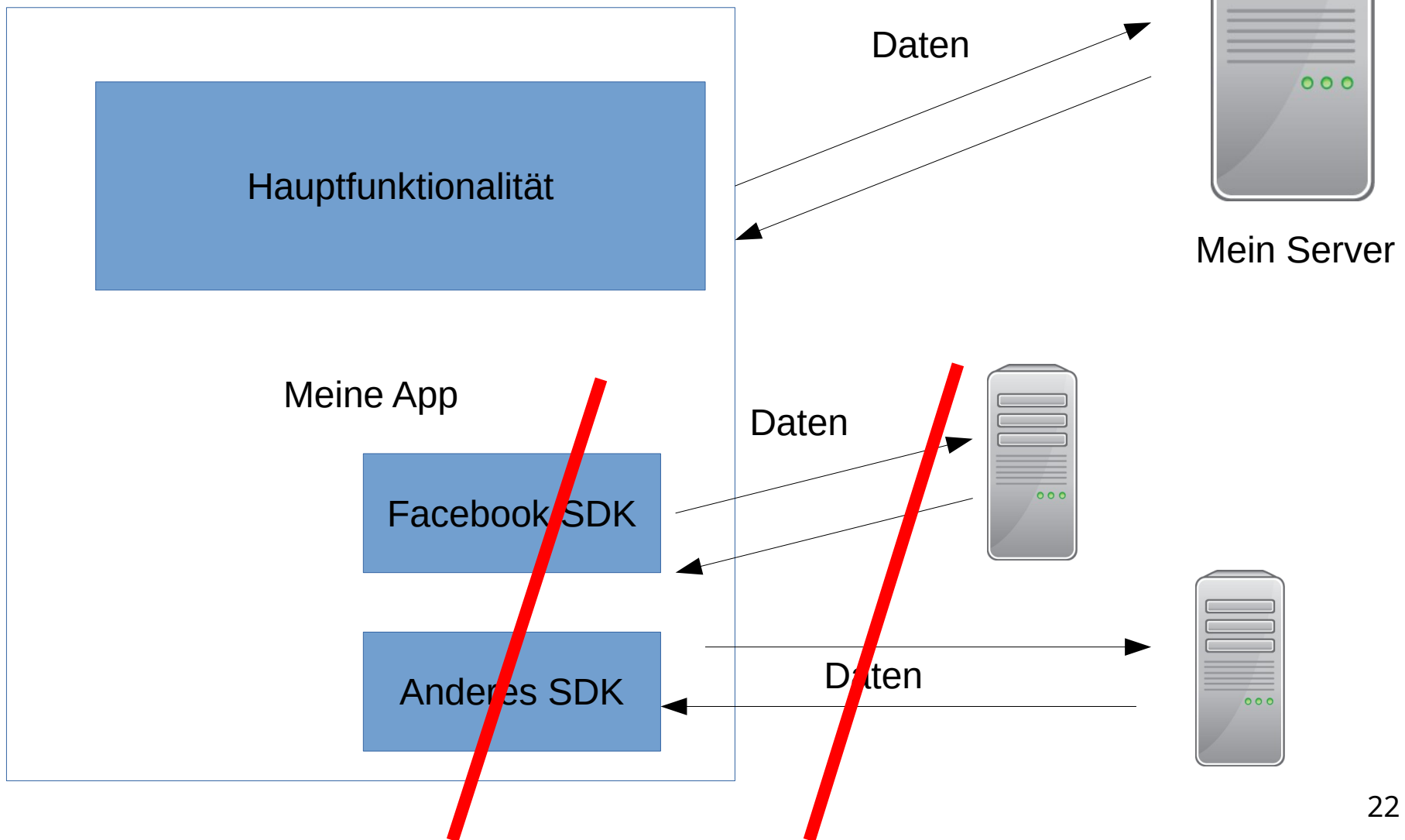
# Personalisierte Werbung



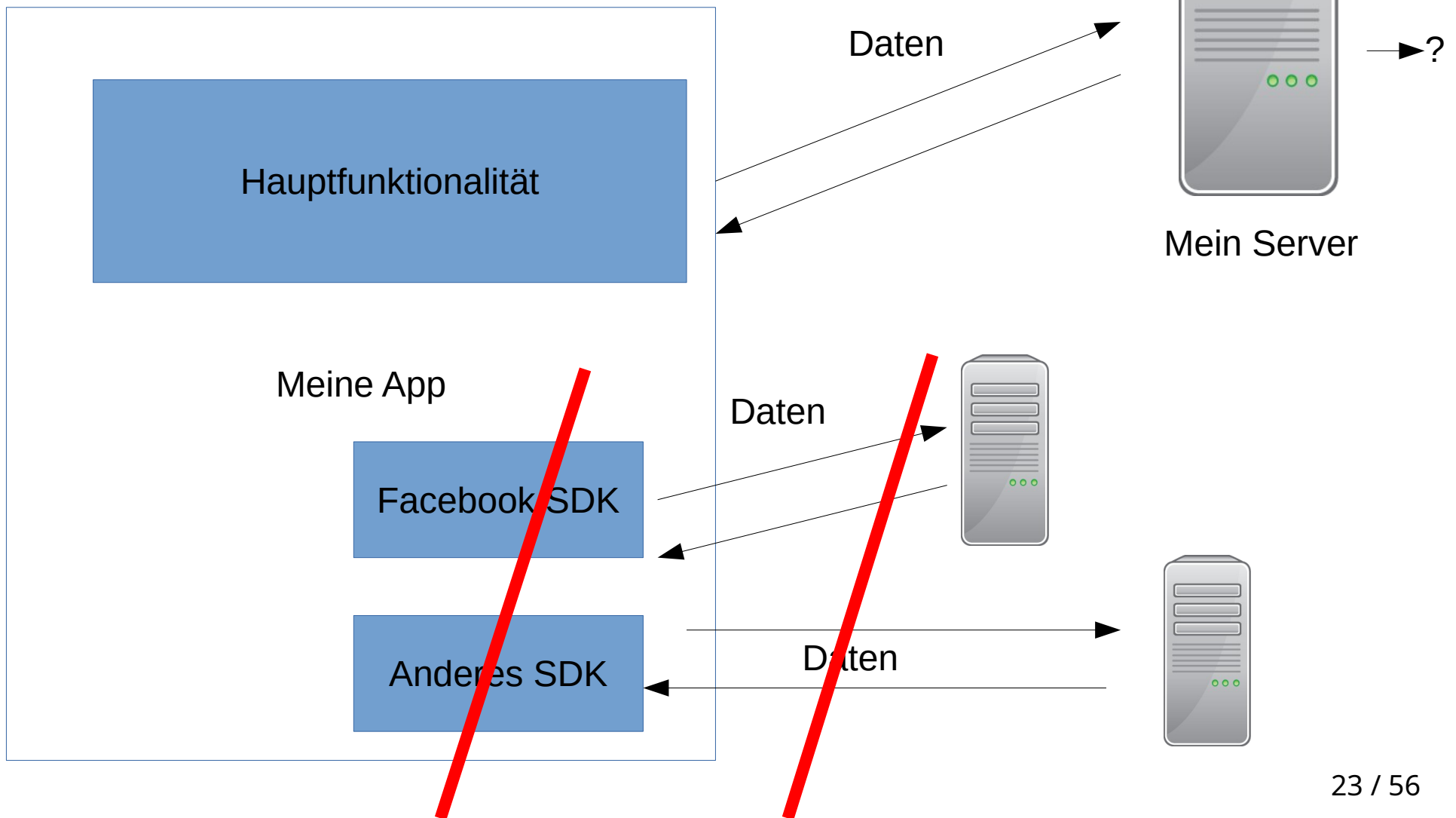
# Personalisierte Werbung



# 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

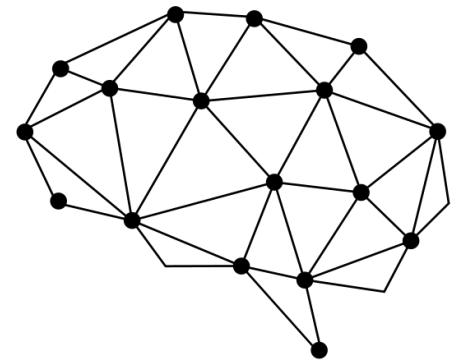
- Beispiel: Schufa Holding AG
  - Daten kommen von Vertragspartnern (z.B. Bank bei der dein Konto liegt, Versandhandel)
  - Je höher Score, desto höher wird Kreditwürdigkeit eingeschätzt
  - Algorithmus nicht bekannt
- Art. 15 Abs. 1 lit h DSGVO:
  - Offenlegung „aussagekräftige[r] Informationen über 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 \*

# Bonitätsbeurteilungen

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

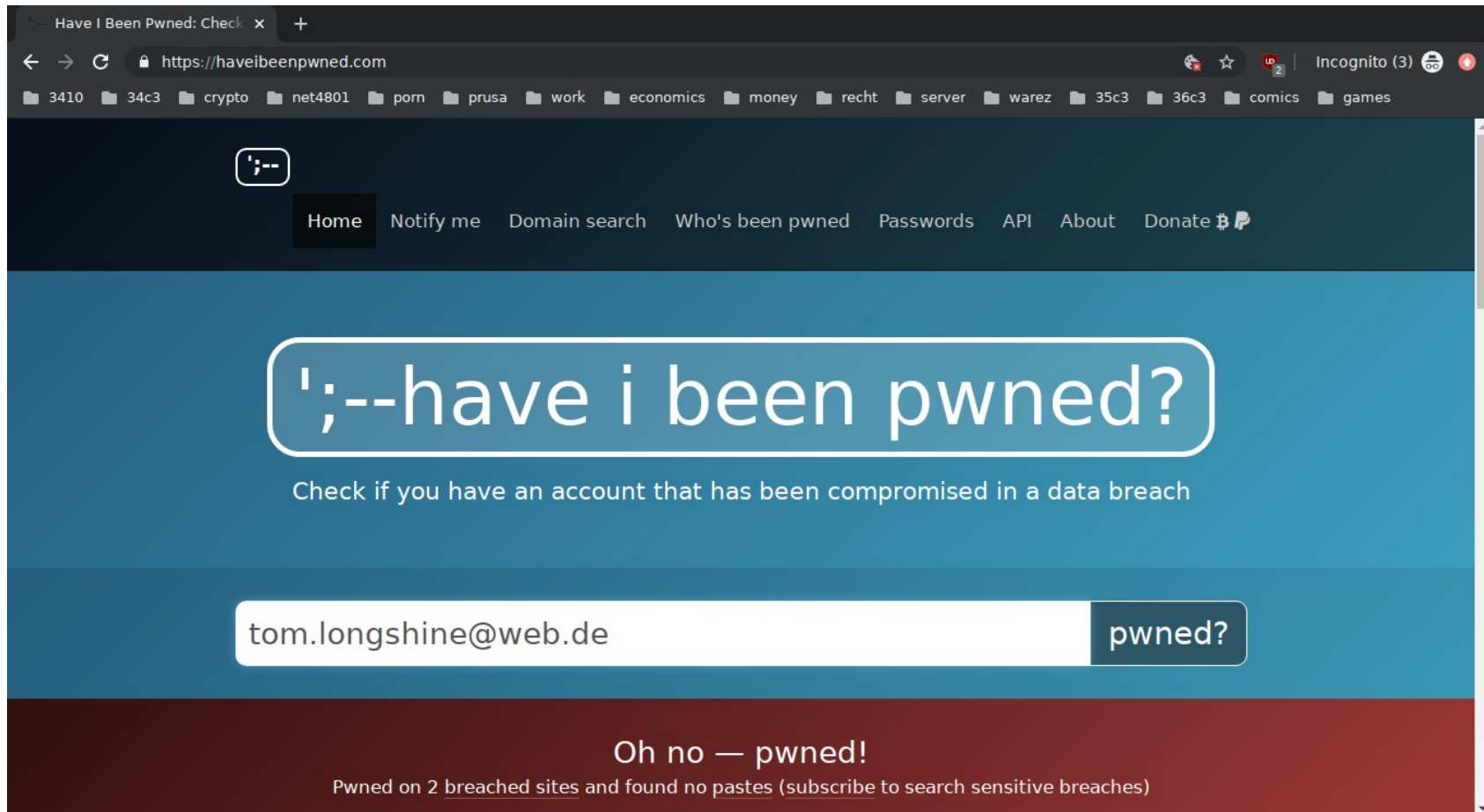
# Cambridge Analytica

- Individualisierte Werbung?  
→ 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 ...



The screenshot shows a web browser window with the URL `https://haveibeenpwned.com`. The browser's address bar and tabs are visible at the top. The website's navigation menu includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area features a large search box with the text `';--have i been pwned?` and a subtext: `Check if you have an account that has been compromised in a data breach`. Below this, a search input field contains the email address `tom.longshine@web.de` and a button labeled `pwned?`. The bottom section of the page displays the result: `Oh no — pwned!` followed by `Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)`.

# “Datenreichtum” bei Unternehmen ...


Have I Been Pwned: Check x +

https://haveibeenpwned.com


3410 34c3 crypto net4801 porn prusa work economics money recht server warez 35c3 36c3 comics games

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

 **Dropbox:** In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

**Compromised data:** Email addresses, Passwords

 **Roll20:** In December 2018, the tabletop role-playing games website Roll20 suffered a data breach. Almost 4 million customers were impacted by the breach and had email and IP addresses, names, bcrypt hashes of passwords and the last 4 digits of credit cards exposed. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Email addresses, IP addresses, Names, Partial credit card data, Passwords

|                |                |         |                |
|----------------|----------------|---------|----------------|
| 438            | 9,555,428,218  | 111,901 | 134,941,789    |
| pwned websites | pwned accounts | pastes  | paste accounts |

# ... führt zu Reichtum bei Scammern

The screenshot displays a marketplace interface with a sidebar for browsing categories and a main area showing a list of items for sale. The items are sorted by price from low to high.

**BROWSE CATEGORIES**

- Fraud 4631
- Accounts & Bank Drops 1670
- CVV & Cards 985
- Dumps 196
- Other 623
- Personal Information & Scans 1157
- Drugs & Chemicals 33155
- Guides & Tutorials 3330
- Counterfeit Items 2630
- Digital Products 6774
- Jewels & Gold 727
- Carded Items 312
- Services 466
- Other Listings 384
- 506

Sort: Price Low to High - Price High to Low

**[sticky] Non vbv VISA CARD 1k - 5k HIGH BALANCED credit card CVV (Buy 1 get 1 FREE)**  
Item # 92863 - Fraud / CVV & Cards - money007 (2373)  
Views: 48893 / Sales: 1143  
Quantity left: Unlimited  
Buy Price: EUR 3.68 (0.000551 BTC)

**[sticky] [SUPPER OFFER] 2X CREDIT CARD CVV KNOWN BALANCE 1k\$ - 50k\$+UPDATE FRAUD PACK 2020 -BUY 1 GET 1 FREE**  
Item # 93815 - Fraud / CVV & Cards - ixorex (4305)  
Views: 4503 / Sales: 149  
Quantity left: Unlimited  
Buy Price: EUR 9.21 (0.001377 BTC)

**[sticky] \$5,000 TO \$10,000 LIVE CVV CC CREDIT CARD. COMES WITH 7 FREE CASHOUT GUIDES (\$10)**  
Item # 132793 - Fraud / CVV & Cards - pastor411 (1018)  
Views: 3730 / Sales: 289  
Quantity left: Unlimited  
Buy Price: EUR 9.21 (0.001377 BTC)

**[sticky] [SUPPER OFFER] 2X - \$500- \$25,000 Aged Paypal With Bank,CC,Cookie ★High Quality★ 100% LogIn Rate**  
Item # 83049 - Fraud / Accounts & Bank Drops - ixorex (4305)  
Buy Price: EUR 32.23 (0.004819 BTC)

# 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



Dimitrios Johann - Fake Na x +

https://namefake.com/german\_germany/random/7580dcefad2917701e81a97fd358a3e2

3410 34c3 crypto net4801 porn prusa work economics money recht server warez 35c3 36c3 comics games

## Fake Name Generator

Name

Gender  male

---

### Dimitrios Johann

Giorgio-Gehring-Platz 82 09418 Mühl Dorf Inn  
**Geo coordinates** -80.789144,14.176451  
**Mother's maiden na...** Jäntsch

**Birthday**

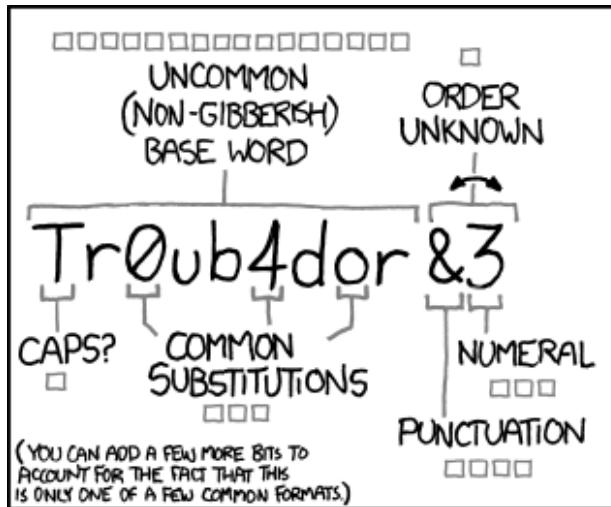
|               |              |
|---------------|--------------|
| <b>Date</b>   | 1983-06-30   |
| <b>Age</b>    | 36 years old |
| <b>Zodiac</b> | Cancer       |

**Phone**

|                   |                   |
|-------------------|-------------------|
| <b>Home phone</b> | 03539 216106      |
| <b>Work phone</b> | +49(0)4488 881841 |

**Internet**

# Passwörter



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

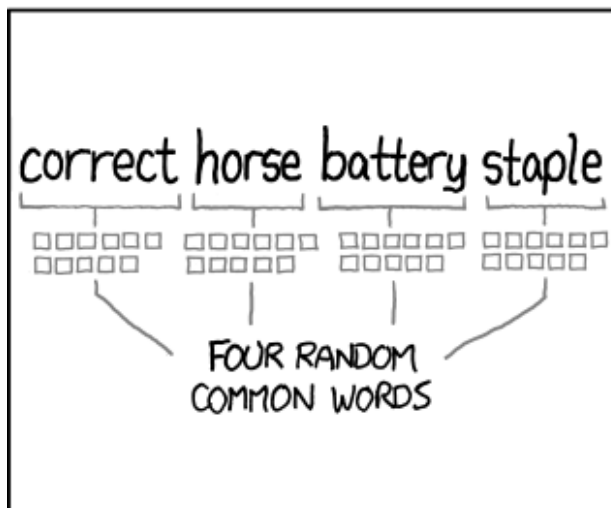
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

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

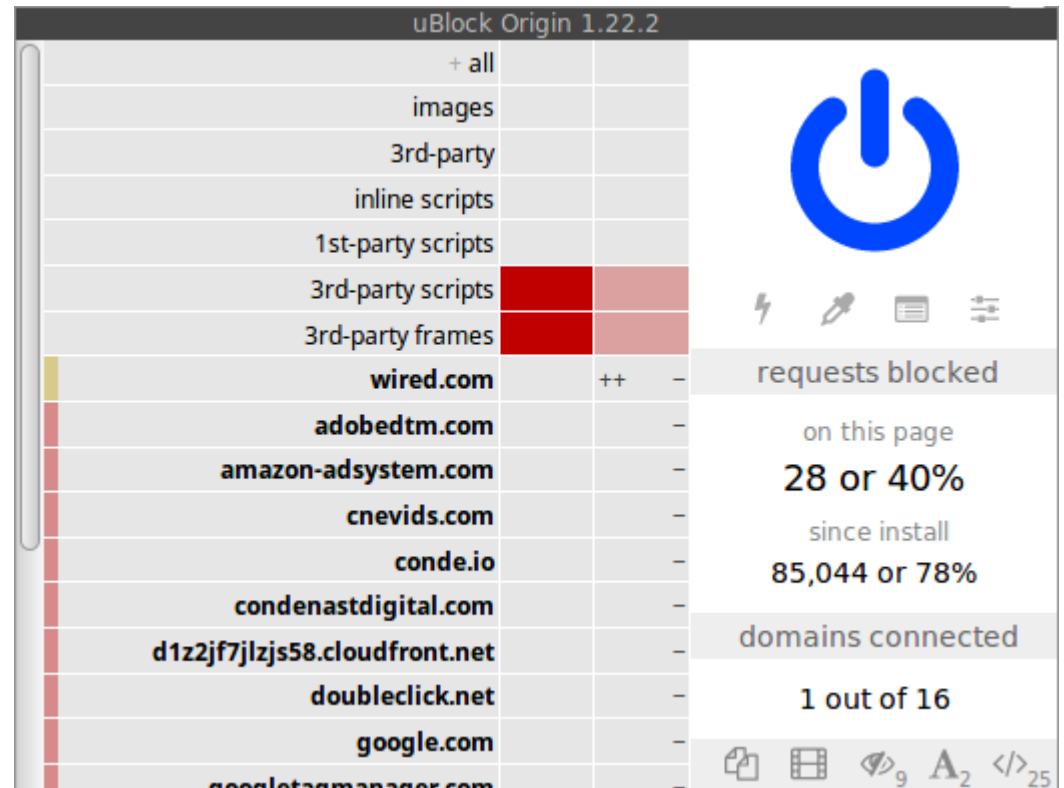
- Muss ich wirklich?
  - Ja.
- Kann es sein, dass dadurch Dinge kaputt gehen?
  - Sollte nicht, aber leider nicht komplett auszuschließen :(

# 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



## You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

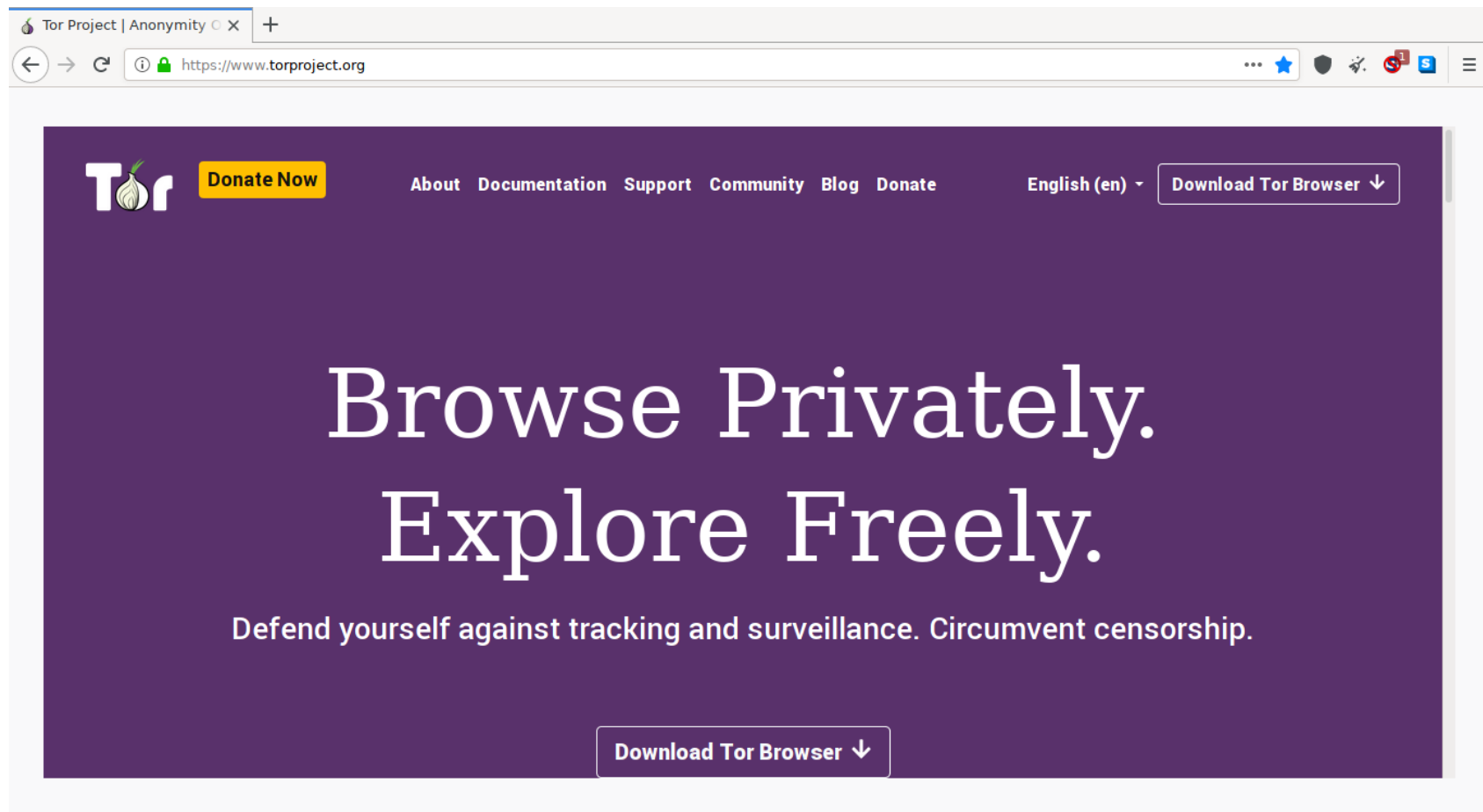
Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

# Tor Browser



# Verschlüsselung

|               | WhatsApp | Facebook | Threema | Telegram | Signal | Wire | Conversations | Briar | Deltachat |
|---------------|----------|----------|---------|----------|--------|------|---------------|-------|-----------|
| Open Source   | -        | -        | -       | +        | +      | +    | +             | +     | +         |
| Crypto        | +        | -        | +       | ~        | +      | +    | +             | +     | +         |
| Infrastruktur | -        | -        | -       | -        | -      | -    | +             | +     | +         |
| Desktop       | ~        | +        | -       | +        | ~      | +    | +             | -     | +         |
| "Features"    | +        | +        | +       | +        | ~      | +    | ~             | -     | ~         |

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

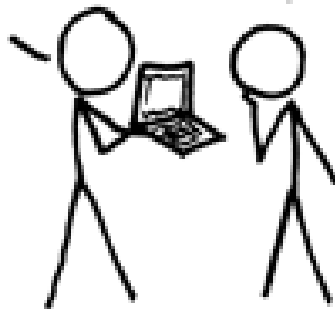
# Technologie vs. Politik

A CRYPTO NERD'S  
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.  
LET'S BUILD A MILLION-DOLLAR  
CLUSTER TO CRACK IT.

BLAST! OUR  
EVIL PLAN  
IS FOILED!

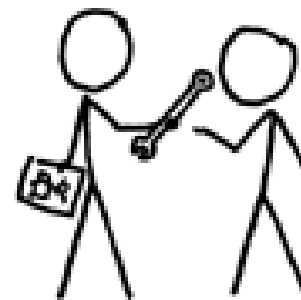
NO GOOD! IT'S  
4096-BIT RSA!



WHAT WOULD  
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.  
DRUG HIM AND HIT HIM WITH  
THIS \$5 WRENCH UNTIL  
HE TELLS US THE PASSWORD.

GOT IT.



# 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!