

BigBlueButton - Startram - Mozilla Firefox

https://bbb.teckids.org/html5client/join?se ... site:kuketz-blo

NACHRICHTEN

Öffentlicher Chat

NOTIZEN

Geteilte Notizen

TEILNEHMER (2)

Sy Sylvia Lange (Sie)

Al Alice

(short) tutorial videos.

To join the audio bridge click the phone button. Use a headset to avoid causing background noise for others.

This server is running BigBlueButton.

To join this meeting by phone, dial: +49 228 30402085  
Then enter 30567 as the conference PIN number. To mute or unmute, press 0.

Um jemanden zu schicken Sie ihm https://bbb.teck

Chat: Fragen stellen

Teilnehmer, auf eigenen Namen klicken um Hand zu heben

Mikro an / aus

Teilnehmersymbole links

Am unteren Rand

Mikro an / aus (muten)

Webcam an / aus

Bildschirm teilen

Präsentation größer anzeigen

Teilnehmer ohne Mikro

Teilnehmer mit Mikro, eingeschaltet

Teilnehmer gemutet (Mikro aus)

Nachrichte senden an Öffentlicher Chat

# Cryptoparty für Anfänger

Ein Einstieg in die Welt der digitalen Selbstverteidigung

Sylvia Lange

7.5.2022

1 Begriffe

2 Gegenmaßnahmen

3 Für die UserIn

# Fragen?

- Es gibt keine dummen Fragen!
- Verständnisfragen bitte direkt.
- Alle anderen Fragen im Anschluss an den Vortrag.

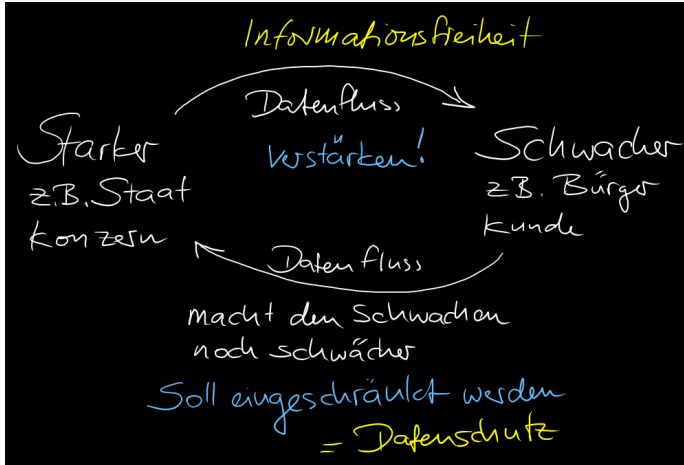
# Sylvia Lange

- Lehrerin für Informatik (Oberstufe am Beruflichen Gymnasium)
- Mitglied des Chaos Computer Club
- Beschäftigung mit Datenschutzthemen in der Freizeit, z.B. bei Events des CCC

## Disclaimer

- Die Autorin ist weder IT-Sicherheits-Expertin noch Juristin.
- Die Informationen veralten schnell.

# Datenschutz und Informationsfreiheit



# Begriffsklärung – zwei Arten von Schutzzielen

Umweltschutz,  
Artenschutz,  
Informantenschutz,  
Jugendschutz,  
Mutterschutz,  
Landschaftsschutz

Virenschutz,  
Sonnenschutz,  
Lärmschutz,  
Feuerschutz,  
Erosionsschutz,  
Kälteschutz,  
Wärmeschutz  
Hochwasserschutz,  
Kündigungsschutz,  
Blitzschutz

# Was ist Datenschutz?

Datenschutz ist nicht der Schutz  
**von Daten**, sondern der Schutz  
**von Menschen vor dem**  
**Missbrauch von Daten.**



# Zum Nachdenken

Warum darf ein Arbeitgeber beim Bewerbungsgespräch nicht nach der Familienplanung fragen?

Warum gibt es die ärztliche Schweigepflicht?

# Missbrauchspotenzial durch Daten

- Diskriminierung (z.B. Arbeitsmarkt, Preisdiskriminierung, Preise für Versicherungen)
- Manipulation (z.B. Microtargeting, bei Wahlen, siehe Cambridge Analytica)
- Unterdrückung von Opposition
- ungesunde Marktmacht (z.B. Thema KI und autonomes Fahren)

Video von mobilsicher zu den Gründen für Datenschutz:

<https://peertube.mobilsicher.de/w/qjKXZJfij9wVvBQscMbcqy>

# Problem der Datenhäufung

- Größere Datensammlungen sind mehr als die Summe der Einzelteile.  
Aus vielen, vielen an sich harmlosen Daten setzt sich ein Gesamtbild der Persönlichkeit und des Gesundheitszustandes zusammen.
- Große Datensammlungen sind ein **Marktvorteil**. Ein kleines Startup könnte nie eine KI für autonomes Fahren bauen.
- Kartellämter haben einen Sinn: Im Kapitalismus ist es problematisch, wenn **einzelne Player zu mächtig** werden. Häufungen von Daten sind gefährlich.

# Gegenmaßnahmen auf Userseite

- bestimmte Dienste meiden
- insbesondere Dienste meiden, die Zustimmung zu langen und unverständlichen AGB verlangen
- Ende-zu-Ende-Verschlüsselung nutzen!

**ABER:** Der Schutz auf Userseite hat deutliche Grenzen! Schutz der Bürger durch Politik nötig!

# Politische Gegenmaßnahmen: Die DSGVO

- DSGVO = Datenschutzgrundverordnung der EU
- politischer Durchbruch wegen **Marktortprinzip**:  
Es gelten die Gesetze der EU, wenn ein Produkt in der EU angeboten wird. Egal wo der Firmensitz des Unternehmens ist.
- sehenswerte Reportage über den politischen Prozess auf EU-Ebene: *Democracy - Im Rausch der Daten*, David Bernet
- **Problem**: geltendes Recht muss umgesetzt werden, siehe BBA 2022 für Irische Datenschutzbehörde.

<https://bigbrotherawards.de/>

- Schützt Bürger, Konsumenten, **ABER** nur bis zur Zustimmung zu AGB!

# DSGVO und AGB

**Merke:** Ab dem Moment, wo der Kunde zu etwas zustimmt, ist alles legal wozu die Einwilligung gegeben wurde.

DSGVO-konform heißt nur: Der Kunde hat allem, was passiert, zugestimmt.

DSGVO-konform  $\neq$  datensparsam

# Organisationen unterstützen!

Digitalcourage, EDRI, noyb, ...

- machen Lobby-Arbeit, kleiner Gegenpol zu Lobbyisten von Big Tech
- informieren die Öffentlichkeit, z.B. Big Brother Award
- **freuen sich über Spenden**

# Politische Arbeit versus Maßnahmen des Individuums

- Man kann sich nicht komplett gegen Datenabfluss schützen, es sei denn man zieht in den Wald oder eine Höhle und verzichtet komplett auf Technik.
- Man kann aber den Datenabfluss reduzieren.
- Die wichtigste Ebene ist aber die Politische!



# Meine ganz persönliche Empfehlung

**Pareto:** Den eigenen Datenabfluss mit vertretbarem Aufwand auf 20% reduzieren. Lieber regelmäßig für Datenschutz- Organisationen spenden als einen großen Aufwand für Individualmaßnahmen betreiben.

# Was die´ einzelne UserIn tun kann

- faire Messenger benutzen
- datensparsam Surfen (3-Browser-Konzept)
- faire Dienste nutzen
- OpenSource-Software nutzen

# Messenger

## Whatsapp meiden!

- gehört zu Meta (Facebook-Konzern), also Problem der **Datenhäufung**
- Meta kann zwar (vermutlich) nicht den Nachrichten- Inhalt lesen, aber **Metadaten** verraten bereits sehr viel
- **Kontakte** werden zu Meta hochgeladen. Meta hat den größten **Social Graph** der Welt.

- Wer kennt wen?
- Wer ist wichtig?
- Wen muss man von einem Service überzeugen? Wo muss man sich weniger Mühe geben?



# Messenger

## Signal Messenger

- amerikanische Server (also von Patriot Act betroffen)
- spendenbasiert, kostenlos
- zwingend an Telefonnummer gebunden

## Threema

- schweizer Firma, Server in der Schweiz
- kostet einmalig ca. 3 €
- muss nicht mit Telefonnummer verknüpft werden

Mein Tipp: Diese beiden Messenger installieren, mit dem Ziel irgendwann Whatsapp deinstallieren zu können.

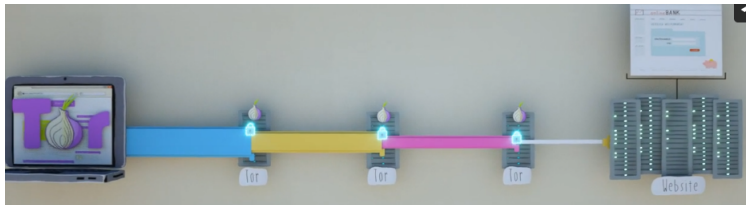
# Datensparsames Surfen: Das 3-Browser-Konzept

- 1 TOR-Browser für alles außer Seiten, auf denen man sich einloggt. (Aus Ökogründen auch keine Videos, Downloads großer Dateien)
- 2 Browser, z.B. Firefox, mit
  - **Addons gegen Tracking**, z.B. uBlock Origin) und
  - **Addons für das Löschen von Cookies** (z.B. Cookie Autodelete)
- 3 Browser ohne Trackingschutz für Seiten, für die der Browser 2 nicht funktioniert

## Erklärung des 3-Browser-Konzepts

[https://www.kuketz-blog.de/  
das-3-browser-konzept-not-my-data-teil2/](https://www.kuketz-blog.de/das-3-browser-konzept-not-my-data-teil2/)

# Was ist TOR



- Anonymisierungsnetzwerk
- Selbst der Webseitenbetreiber weiß nicht, von welcher IP-Adresse man kommt
- Pakete werden mehrfach verschlüsselt und nehmen zur Verschleierung einen längeren Weg durchs Internet
- Super Erklärvideo: <https://vimeo.com/164049726>

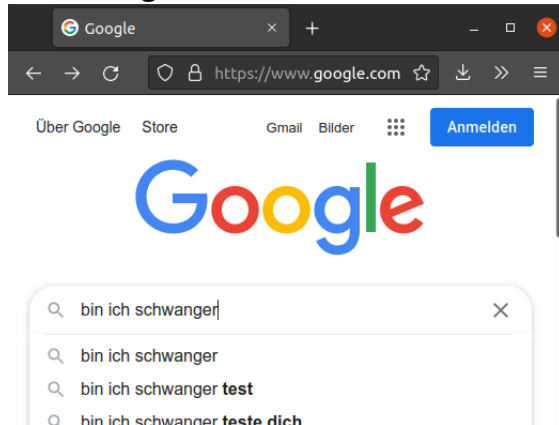
# Auswahl von Diensten: Mail-Provider

- Welches Geschäftsmodell? Zahlen mit Daten oder Zahlen mit kleinem Eurobetrag?
- Z.B. bei gmail (von Google) akzeptiert man das automatisierte Scannen der Mails (z.B. für personalisierte Werbung)
- Gute Alternativen:
  - Posteo (1€ pro Monat)
  - Mailbox.org (1€ pro Monat)
  - Tutanota (auch kostenlos möglich, einfache Verschlüsselung ohne PGP)



# Auswahl von Diensten: Suchmaschine

**Jede Frage an eine Suchmaschine ist eine Antwort.**



■ unbedingt Standardsuchmaschine im Browser ändern. ▶

# Empfehlenswerte Suchmaschinen

- Duckduckgo (amerikanisch)

`https://duckduckgo.com/`

- Metager (deutsch) `https://metager.de/`

- Ecosia (öko) `https://www.ecosia.org`

- Startpage (anonymisierte Google-Ergebnisse)

`https://www.startpage.com/`

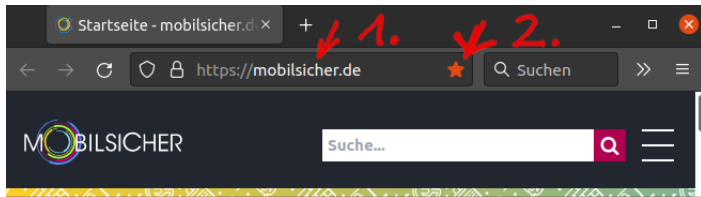
- Qwant (französisch) `https://www.qwant.com/`

`https://mobilsicher.de/ratgeber/`

`suchmaschinen-die-fuenf-besten-alternativen-zu-google`

# Zusätzlich bei Suchmaschinen zu beachten:

- 1 Bekannte Adressen immer in die Adressleiste (ganz oben im Browser) eingeben, nicht in ein Suchfeld – das spart auch Strom
- 2 Lesezeichen setzen für Seiten, die man öfter benutzt



# Auswahl von Diensten: Der Kartendienst Openstreetmaps

- durch Nutzung von Google Maps landen weiter aussagekräftige Daten bei einem großen Player
- gute Alternative ist Openstreetmaps
- im Browser `https://www.openstreetmap.org`
- mobile App OsmAnd+ (Openstreetmaps and More)
- Karten lokal speicherbar, **Navigation ohne Netzeempfang möglich!**

# Auswahl von Diensten: Alternativen suchen

- Dienste, die eine Einwilligung erpressen, meiden!
- nach Alternativen suchen



# Apps auf dem Handy

- Apps immer nur die Berechtigungen erteilen, von denen plausibel ist, dass sie gebraucht werden.
- z.B. braucht eine App für Textbearbeitung sicher keinen Standort
- Nur Apps auf dem Handy haben, die man **wirklich aktuell benötigt**.
- Also immer wieder aufräumen und **nicht mehr benötigte Apps löschen**.
- Vor dem Löschen überlegen: Gibt es einen **Account** beim Anbieter, den man erst noch **löschen** muss?  
Sonst bleiben Daten beim Anbieter.

# Proprietäre Software versus FOSS

## Proprietär:

- Windows, Microsoft Office, alles von Apple ...
- Lock-In-Effekt: NutzerIn investiert Zeit, um sich mit der Bedienung vertraut zu machen. Wird alle Änderungen an den Rahmenbedingungen akzeptieren.
- NutzerIn ist abhängig vom Hersteller
- Produkte senden oft Nutzerdaten an den Hersteller

# Proprietäre Software versus FOSS

## Free and Open Source Software

- Linux, Libre Office, Open Office, Firefox, Thunderbird
- Man muss keine AGB lesen und akzeptieren
- kein Lock-In-Effekt
- Selbst wenn es Änderungen gibt, die man nicht gut findet, kann man auf Forks hoffen: Freiwillige pflegen Versionen der Software in ihrer Freizeit weiter
- Senden von Nutzerdaten kann man in der Regel abwählen



# Die datenbewusste BürgerIn nutzt Linux

Den Umstieg vorbereiten:

- zunächst beim gewohnten Betriebssystem bleiben (z.B. Windows), dort aber immer weiter an Software gewöhnen, die es auch für Linux gibt
- Libre oder Open Office statt MS Word
- Firefox statt Edge
- Thunderbird statt Outlook
- Wenn diese Umgewöhnung geglückt ist, ist der Umstieg auf Linux keine große Hürde mehr.

# Dringende Empfehlung: Passwortmanager

- Passwörter sollten mind. 14 Zeichen lang sein und komplex
- **KEINE Mehrfachverwendung!**
- Lösung: Passwortmanager, z.B. KeepassXC
- Ganze Passwortsammlung wird mit einem sehr langen, sehr sicheren Master-Passwort geschützt
- ABER Achtung: Masterpasswort muss SEHR STARK gewählt werden.

# Gute Informationsquellen

- <https://mobilsicher.de/>
- <https://digitalcourage.de/>
- <https://www.kuketz-blog.de/>
- **Konkrete Softwareempfehlungen**  
<https://www.cryptoparty.in/learn/tools>

# Danke für die Aufmerksamkeit!

## ■ Download der Folien:

`https://raw.githubusercontent.com/  
sylvialange/vortraege/main/beginner.pdf`