

# SICHER IM NETZ

Online-Workshop zu Online-  
Privatsphäre und Datensicherheit

# ABLAUF

- Was ist uns wichtig und warum?
- Was können wir tun?
  - *6 Schritte zur Online-Selbstverteidigung*

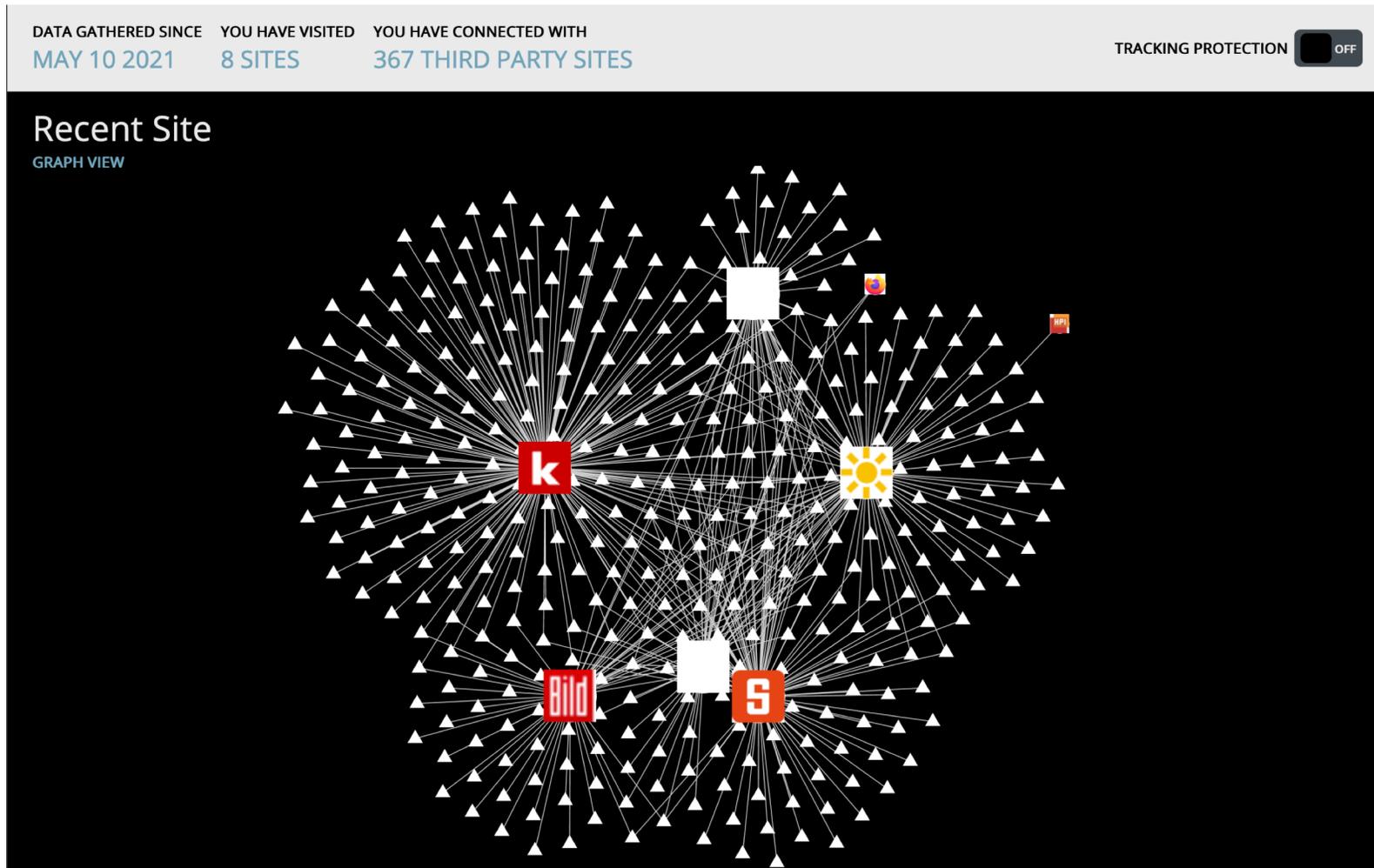
# WELCHEN AKTEUR NIMMST DU ALS GRÖßTE GEFAHR WAHR?

1. Regierungen / staatliche Akteure
2. Cyberkriminelle
3. Unternehmen

# WAS IST DEIN „THREAT MODEL“ (GEFAHRENMODELL)?

- **Assets:** Welche Daten will ich schützen?
- **Threats:** Wer bedroht mich wie?
- **Likelihood:** Wie wahrscheinlich ist ein Angriff?
- **Willingness:** Welche Bereitschaft, habe ich, etwas zu verändern?
- **Consequences:** Was sind Konsequenzen, nicht zu handeln?

# ALLTÄGLICHE EINGRIFFE IN UNSERE PRIVATSPHÄRE



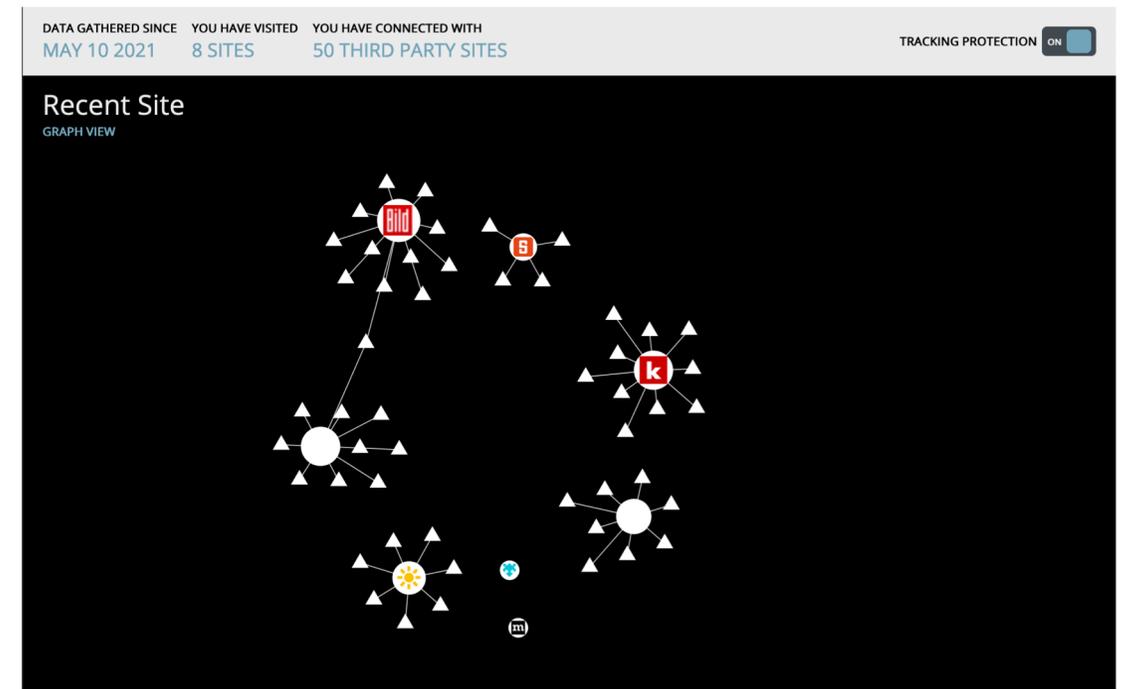
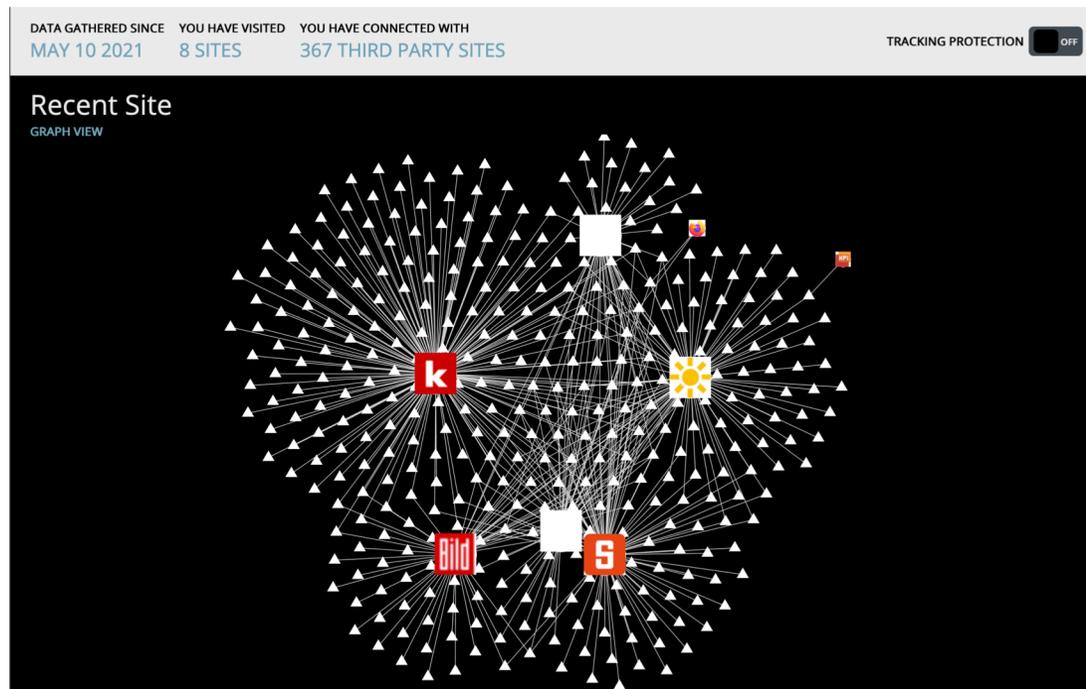
# 1: PRIVATSPHÄRE DURCH ERWEITERUNGEN SCHÜTZEN

- Installiert **Anti-Tracking-Erweiterungen**
- Passt eure **Browser-Einstellungen** an
  - *Drittanbieter-Cookies, Do-Not-Track, Löschen beim Schließen*
- **Widerspricht** der Nutzung von Cookies
  
- Installiert eine **Ad-Block-Erweiterung**
- Installiert **HTTPS Everywhere**

# LIGHTBEAM – VORHER UND NACHHER

367 verknüpfte Tracker

50 einzelne Tracker



# 2: KONTEN SCHÜTZEN

- Betroffen? HPI identity leak checker: <https://sec.hpi.de/ilc/>

## Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [REDACTED] taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.

Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
8tracks.com	Jun. 2017	✓	17.973.604	Betroffen	-	-	-	-	-	-	-	-
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	-	-	-	-	-	-	-	-

Betroffen: Diese Daten wurden in der zum angegebenen Zeitpunkt veröffentlichten Identitätsdatenbank der jeweiligen Quelle gefunden.

-: Es wurden keine solche Daten gefunden.

## 2: KONTEN SCHÜTZEN

### ■ Passwortmanagement

- Passwortmanager für Großteil der Passwörter
  - (*KeepassX vs. Dashlane*)
- Die wichtigsten Passwörter: physisch aufschreiben?
- From PW to Passphrase: Ein langes PW, aber abänderbar

### ■ Setzt **2-Faktor-Authentifizierung** bei wichtigen Konten ein

# 3: DIVERSIFIZIERUNG

- Nutzt verschiedene Browser, Suchmaschinen und E-Mailkonten
  - *Z.B. zwei Browser für "normales" Surfen und soziale Medien*
  - *Z.B. DuckDuckGo als Standardsuchmaschine, Google ab und an*
- **Verschweigt Informationen!** Nutzt anonyme Konten und Pseudonyme
  - *Z.B. Guerrillamail oder blur.me*
- Nutzt Anbieter, die Datenschutz wichtig nehmen
  - *Z.B. Posteo, Mailbox, Protonmail*

## 4: BACKUPS ZUR SICHERUNG DER DATEN

- Smartphones auf dem Rechner oder in der Cloud
- Rechner auf externer Festplatte oder Cloud

## 5: EINE INVENTUR MACHEN

- Welche Daten besitzen Unternehmen?
  - *Z.B. Selbstauskunft.net*
  - *Z.B. Google Dashboard, Facebook-Daten herunterladen*
  - *Welche Konten braucht es noch?*
- Privatsphäreinstellungen überprüfen und anpassen
  - *Rechner → Einstellungen Privatsphäre und Sicherheit*
  - *Onlinedienste & Accounts*

## 6: DAS SMARTPHONE SICHERN

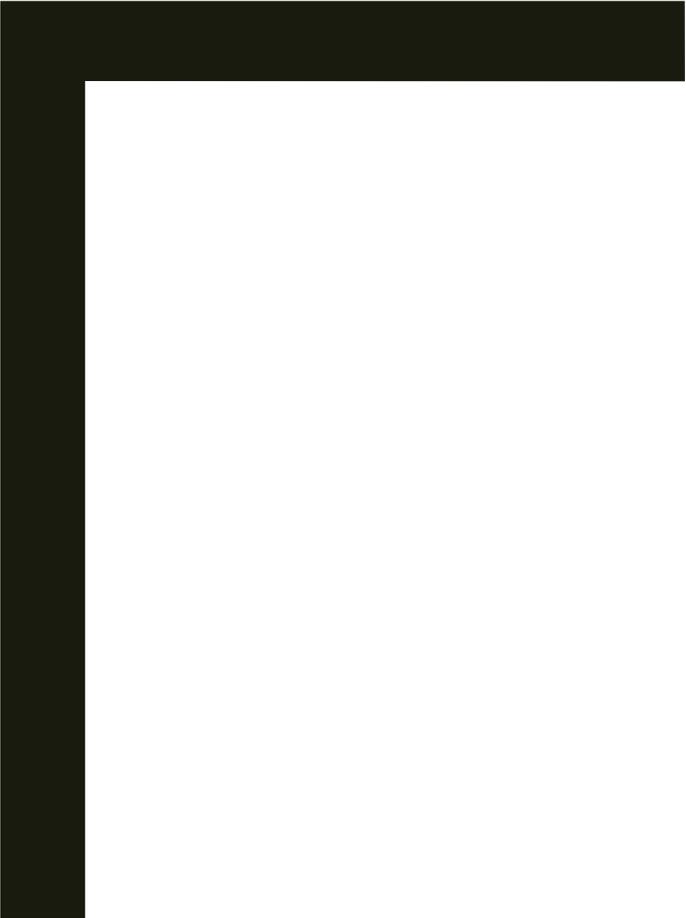
- Verschlüsselt die Daten auf eurem Handy
- Nutzt Browser mit guten Privatsphäre-Einstellungen
  - *Z.B. Firefox, Brave, DuckDuckGo*
- Ändert die Cookie-Einstellungen
- Nutzt andere Suchanbieter
- Nutzt sichere Messenger-Dienste
- Ändert die Privatsphäre-Einstellungen
  - *z.B. Ortungsdaten*

# 7: VERSCHIEDENES

- Virenschutzprogramm
  - Macbooks: Nicht notwendig
  - Windows: Vielleicht
    - Kostenlose Programme sind wenig hilfreich
    - *Empfohlen: Kaspersky, BitDefender, Avast*
  - Wichtiger: Updates automatisch installieren, Backups
- VPN-Dienste & TOR-Browser
  - Gezielt einsetzen, v.a. in öffentlichen Netzen

# WEITERFÜHRENDE LEKTÜRE

- Deutschland Sicher im Netz: <https://www.sicher-im-netz.de/>
- BSI für Bürger: [https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen\\_gegen\\_Internetangriffe.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html)
- Datenwache: <https://www.datenwache.de/tipps-sichere-daten-datenschutz-privatsphaere/>
- GPPi Privacy Toolbox (EN): <https://www.privacytoolbox.gppi.net/obscure-me>
- Security in a Box (EN): <https://securityinabox.org/>
- Digital First Aid (EN): <https://digitaldefenders.org/digitalfirstaid/>
- Kryptoparty (EN): <https://www.cryptoparty.in/learn/tools>
- Remote Working Tools (EN) <https://tacticaltech.org/#/news/technology-is-stupid>



Vielen Dank!



## Creative Commons

Dieser Workshop basiert auf der Website: „[Obscure Me: A Toolbox for Online Privacy](#)“ des [Global Public Policy Institutes](#) (GPPI). Die Inhalte wurde übersetzt, aktualisiert und um Anwendungen ergänzt. Dieses Werk ist ebenfalls lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 3.0 Unported Lizenz](#).

Alle Angaben ohne Gewähr.