



# Let's Kryptoparty!

Kleines Fest der informationellen Selbstbestimmung

Markus Kiunke und Aleksander Paravac

<https://www.nerd2nerd.org>

# Übersicht

1. [Einleitung](#)
2. [Allgemeines](#)
3. [Software](#)
4. [Metadaten](#)
5. [Smartphones](#)
6. [E-Mail](#)
7. [Rechner absichern](#)
8. [Social Media](#)
9. [Anleitungen und Links](#)

# Einleitung

# Schützen? Wovor?

- Firmen
- Ungewollte Software
- Staat



Von: <https://www.youtube.com/user/TheWikiLeaksChannel>

## GCHQ

**Owen Bowcott** *Legal affairs correspondent*

✉ @owenbowcott

Thu 13 Sep 2018 18:16 BST



6,323

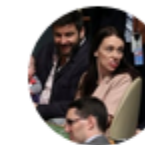
## GCHQ data collection regime violated human rights, court rules

**Surveillance system revealed by Snowden breached right to privacy, Strasbourg judges say**

▲ The GCHQ building in Cheltenham. Photograph: GCHQ/PA

GCHQ's methods for bulk interception of online communications violated privacy and failed to provide sufficient surveillance safeguards, the [European court of human rights](#) has ruled.

## most viewed



Jacinda Ardern makes history with baby Neve at UN general assembly



Weetabix wars: dozens of boxes of British cereal to be destroyed in New Zealand



'The people's yogi': how Adriene Mishler became a YouTube phenomenon



Thailand: three men arrested over murder of British millionaire and wife



Instagram co-founders resign to explore 'creativity again'

# Bin ich schon betroffen?

- [';-have i been pwned?](#)

5.419.217.471 pwned accounts

# Ungewollte Software

- Malware
- Phishing
- Tracking

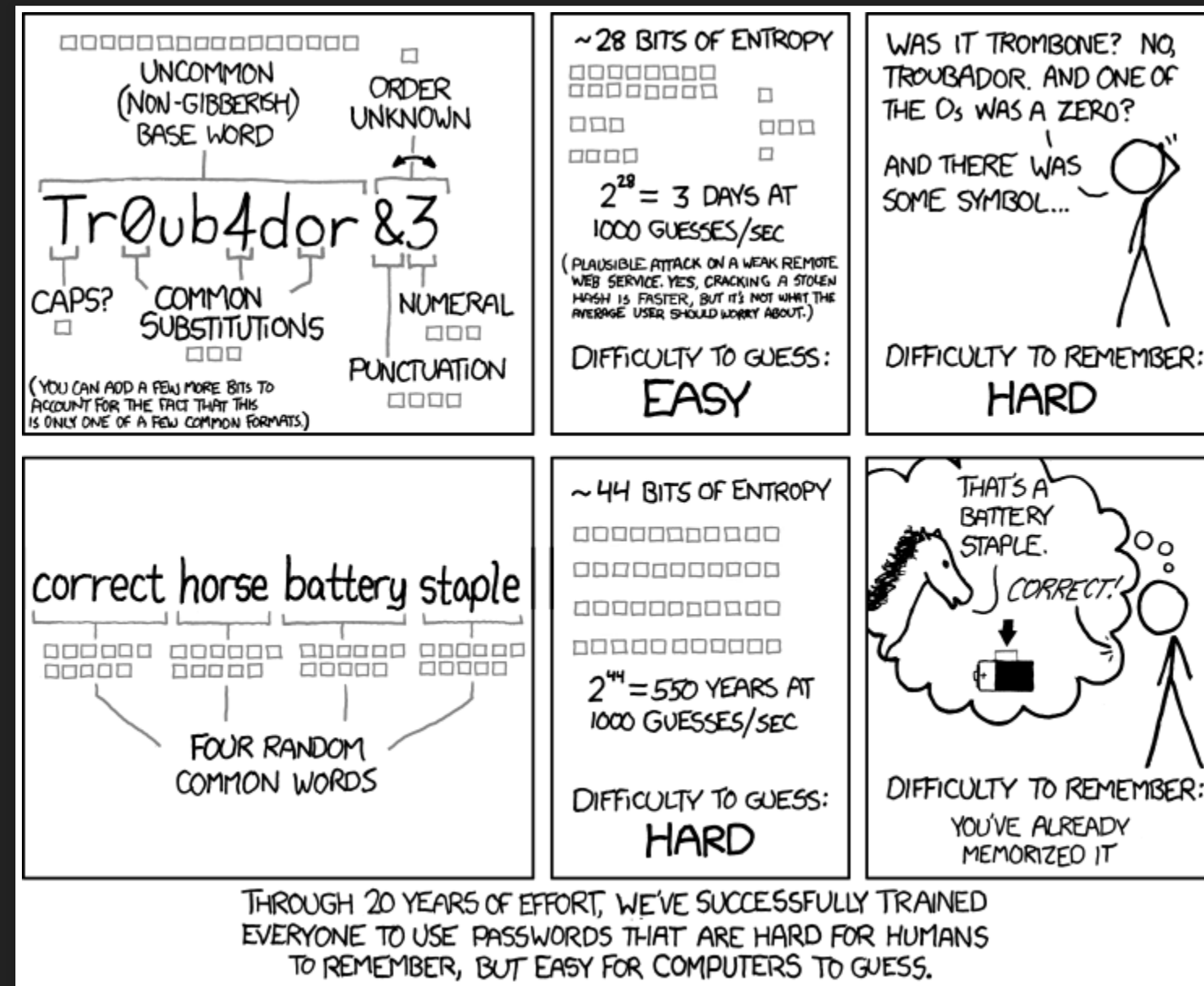


# Allgemeines

- Sichere Passwörter
  - Pro Dienst eines!
  - Passwort-Safes
- Two Factor Authentication
- Ende-zu-Ende-Verschlüsselung

# Beispiel

## Passwort sicher?

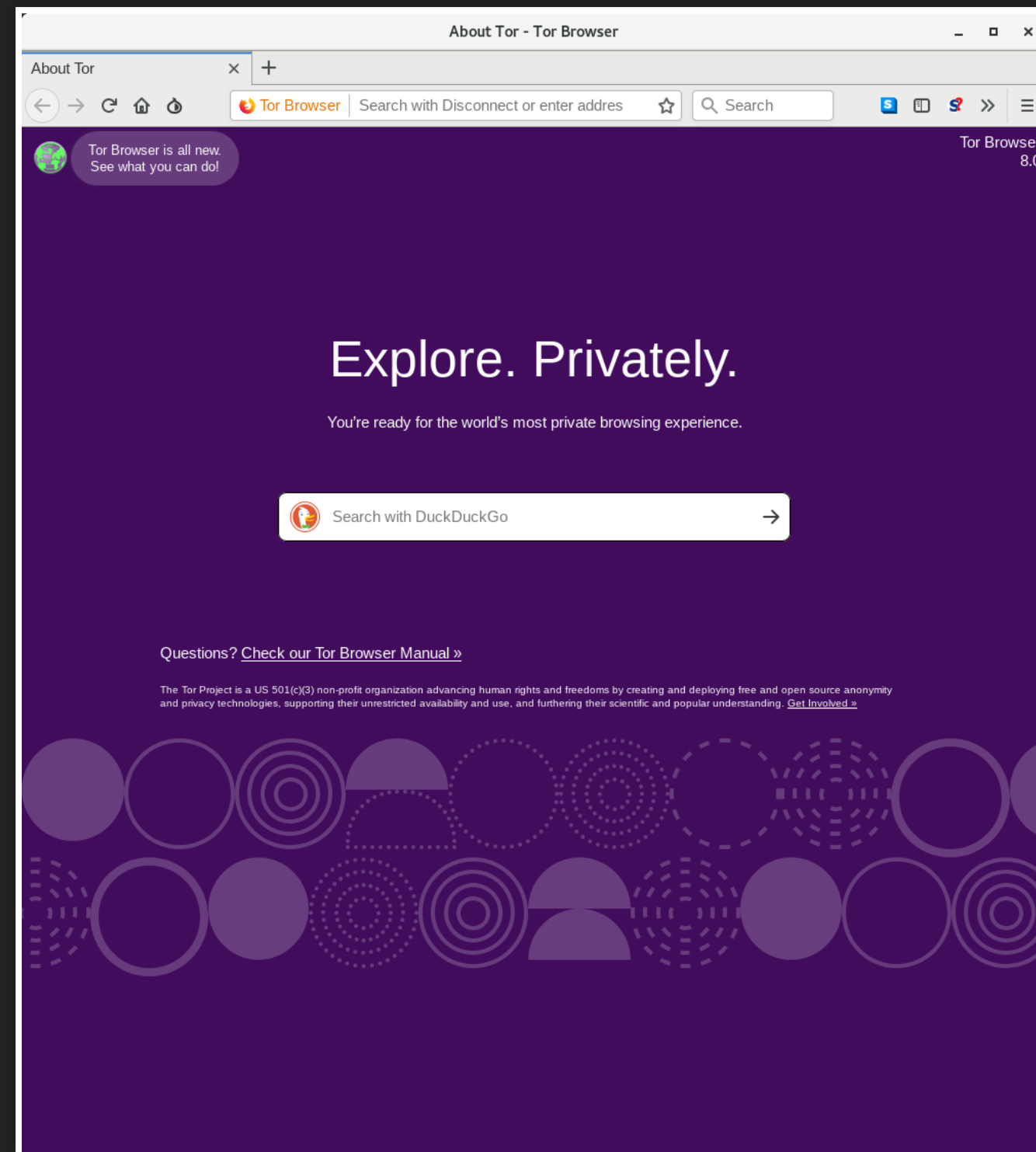


Danke an [XKCD](#).

# Software

- Virens Scanner
- VPN
- Torbrowser
- Updates/Updates/Updates!

# Torbrowser



# VPN?

- VPN Dienst verwenden
- Vertrauen in den VPN-Dienstleister?

# Browser

- [Noscript](#) (Firefox)
- [uBlock](#) (Firefox/Chrome)
- [uMatrix](#) (Firefox/Chrome)
- [Stealthy](#) (Firefox/Chrome)
- [httpseverywhere](#) (Firefox/Chrome)

# Suchmaschinen

- [DuckDuckGo](#)
- [Startpage](#)
- [Disconnect Search](#)

# Metadaten

- Affiliate Networks
- Tracking
- Sicherheit der Cloud Provider



# Smartphones

- Crpyto-Messenger
- Virensscanner?

# Crypto-Messenger

- Whatsapp
- Signal
- Telegram
- Threema
- XMPP (mit OTR/OMEMO/PGP)
  - Chatsecure (iOS)
  - Conversations (Android)

# Signal

## Terms of Use

[SUPPORT](#)[BLOG](#)[DEVELOPERS](#)[JOBS](#)

**Managing your information.** You can manage your personal information in Signal's application Settings. For example, you can update your profile information or choose to enable additional privacy features like a Registration Lock PIN.

### Information we may share

**Third Parties.** We work with third parties to provide some of our Services. For example, our Third-Party Providers send a verification code to your phone number when you register for our Services. These providers are bound by their Privacy Policies to safeguard that information. If you use other Third-Party Services like YouTube, Spotify, Giphy, etc. in connection with our Services, their Terms and Privacy Policies govern your use of those services.

### Other instances where Signal may need to share your data

- To meet any applicable law, regulation, legal process or enforceable governmental request.
- To enforce applicable Terms, including investigation of potential violations.
- To detect, prevent, or otherwise address fraud, security, or technical issues.
- To protect against harm to the rights, property, or safety of Signal, our users, or the public as required or permitted by law.

# Telegram

## Bericht von [Anwaltskanzlei Steiger](#)



[Aktuelles](#) [Profil](#) [Kompetenzen](#) [Publikationen](#) [Medien](#) [Kontakt](#)

---

### Telegram liefert IP-Adressen und Telefonnummern an Sicherheitsbehörden

11. September 2018 · Rechtsanwalt Martin Steiger

Der Messenger Telegram hat in Fachkreisen einen **schlechten Ruf**, ist bei Laien aber eine beliebte Wahl für «sichere» Kommunikation.

Nun sorgt die **Datenschutzerklärung**, die am 14. August 2018 erheblich erweitert wurde, für Aufregung. In der neuen Ziffer 8.3 heisst es ausdrücklich, dass Telegram die IP-Adresse und Telefonnummer von «Terrorverdächtigen» gegenüber Sicherheitsbehörden offenlegen kann:

«If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities.»

Im gleichen Abschnitt schreibt Telegram, das sei bislang noch nie geschehen. Sollte es geschehen, werde man im halbjährlichen Transparenzbericht darüber informieren:

«So far, this has never happened. When it does, we will include it in a semiannual transparency report [...]»

(Bislang ist unter der verlinkten Internet-Adresse <https://t.me/transparency> noch gar kein **Transparenzbericht** vorhanden. Was Telegram unter einer «terrorverdächtigen» Person versteht, wird nicht nicht erläutert.)



#### Kontakt

E-Mail [info@steigerlegal.ch](mailto:info@steigerlegal.ch)

Telefon +41 44 533 13 60  
Telefax +41 44 533 13 61

Steiger Legal AG  
Florastrasse 1  
8008 Zürich  
Schweiz

[Kontaktadressen →](#)

#### Newsletter

Neuigkeiten nicht mehr verpassen:

[Jetzt anmelden](#)

## Telegrams [Privacy Declaration](#)

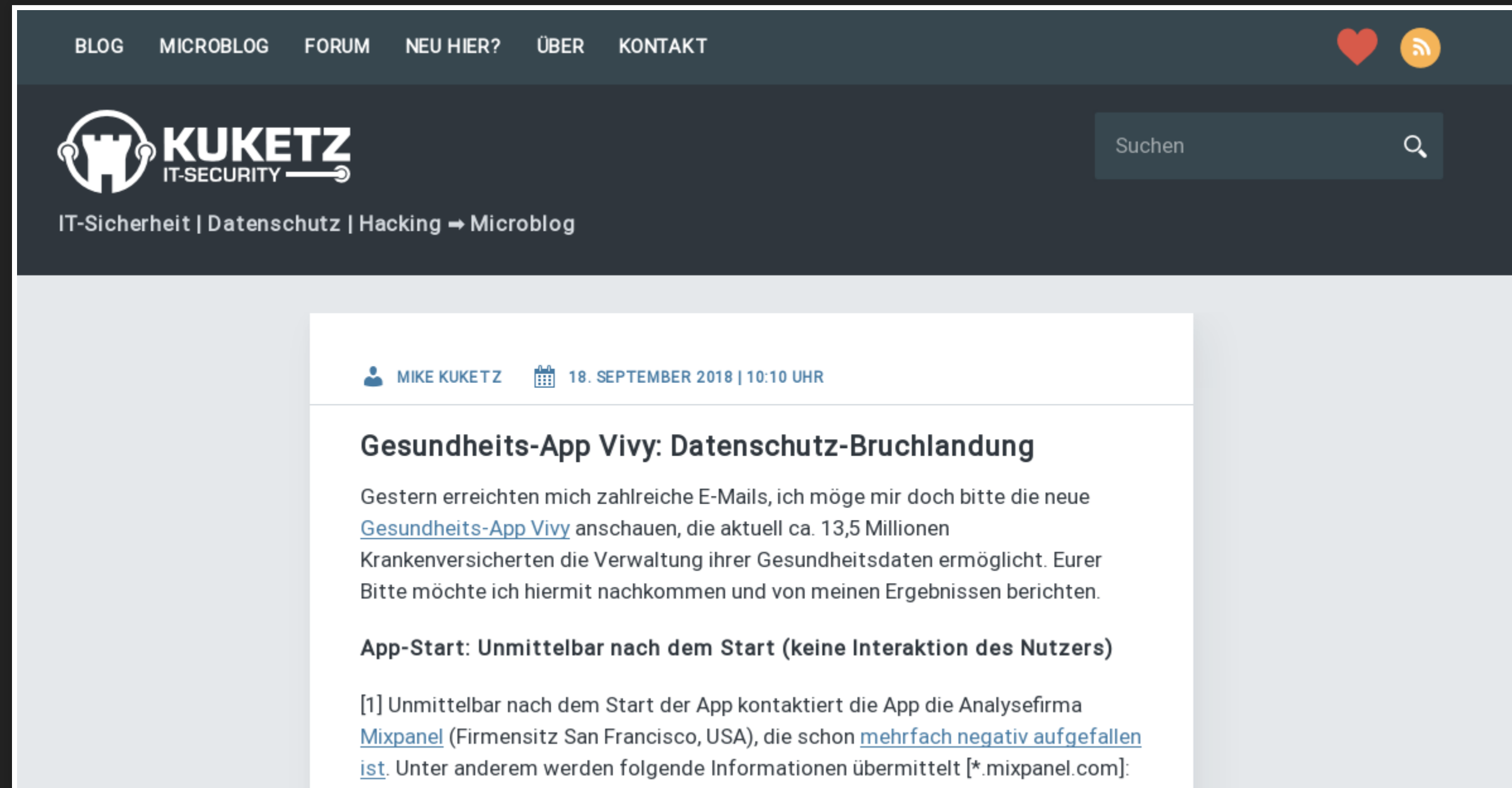
# XMPP

- OTR
- OMEMO
- PGP

# Smarte Apps

- Fitness- und Gesundheitssoftware
- Games
- Finanzapps
- ...

# Gesundheitsapps



Danke an Mike Kuketz

# E-Mail

- “sichere” Mail Provider
  - [Posteo](#)
  - [Mailbox.org](#)
  - [ProtonMail](#)
  - [RiseUp](#)
- PGP (verschlüsselte e-Mails)
  - [Enigmail](#) für Thunderbird
  - [Mailvelope](#) für Firefox
  - [GPG4Win](#) für Outlook



# Rechner absichern

- Keine unnötige Software
- Updates/Updates/Updates
- Quellen überprüfen

# Datenträgerverschlüsselung

- VeraCrypt
- LUKS
- Bitlocker (Aufpassen: Cloud!)

# Social Media

- Facebook
- Instagram
- Twitter
- ...
- you name it
- [mastodon](#)

# Anleitungen und Links

- <https://securityplanner.org/>
- <https://ssd.eff.org/en>

# Videos

- Reihe “Sicher im Netz” von Alexander Lehmann auf [Youtube](#)
- Kurzgesagt: “[Safe and Sorry - Terrorism & Mass Surveillance](#)”
- Arte & BR Dokumentantion: [Do not Track!](#)

# Wo informieren?

- [Electronic Frontier Foundation](#)
- [Netzpolitik.org](#)
- [Chaos Computer Club](#)
- [Digital Courage](#)
- [Deine Daten - Deine Rechte](#)
- [Digitale Gesellschaft](#)

Danke