



Gesellschaft für  
Freiheitsrechte

# It's the incentives, stupid!

„Strategische Verfassungsbeschwerden gegen „Staatstrojaner“ — Wie die GFF für rechtliche Anreize zugunsten der IT-Sicherheit kämpft“

Dr. Ulf Buermeyer, LL.M. (Columbia)

Gesellschaft für Freiheitsrechte e.V.



# Berlin, we have a problem.

„IT-Security“ klingt wie  
„schwarzer Schimmel“

- Bundestag gehackt
- USA: Demokratische Partei im Wahlkampf gehackt
- Berliner Kammergericht monatelang offline



# Bisherige Ansätze verfehlt

## Bisher im Fokus der IT-Sicherheit

- Angreifer / „Hacker“
- Anwender



# Angreifer: nicht greifbar

„Cybercrime“ ist nur in  
Glücksfällen zu bekämpfen

- Täter meist im Ausland
- ineffiziente Rechtshilfe
- Tatbegehung verschleiert
- hochprofessionell (teils staatlich)



# Anwender: überfordert

## Anwender

haben nur begrenzten Einfluss auf ihre Systeme

- Mangel an Expertise
- keine Zugriffsrechte



# Anwender: überfordert

## Anwender

sind Menschen und machen Fehler

- Phishing
- Malware als Email-Anhang ...  
looking at you, Kammergericht!



# Kassensturz

## Zwischenbilanz

- wir setzen an den falschen Stellen an
- nur: welche sind vielversprechend?



# Elephant in the Room

## Die **Hersteller\*** von IT spielen die zentrale Rolle

- treffen sicherheitsrelevante Design-Entscheidungen
- bieten Updates an – oder auch nicht

\*über die Definition muss man reden!





# Problem: Anreizstrukturen

**Hersteller** haben wenig  
Anreize, in Sicherheit zu  
investieren

- Features muss man bauen – Sicherheit kann man behaupten
- Externalisierte Kosten von Sicherheitslücken

# Time is money



Gesellschaft für  
Freiheitsrechte

Hersteller würden mehr in  
Sicherheit investieren, wenn  
es sich **lohnen** würde.



# Time is money

Also müssen wir dafür  
sorgen, dass es sich lohnt.

- Sicherheit als Wettbewerbsvorteil
- Sicherheitsmängel als Kosten-Risiko



# Sicherheit als Wettbewerbsvorteil

## Wettbewerbsvorteile durch **messbare** Sicherheit

- „Mindesthaltbarkeitsdatum“
  - wie lange gibt es Updates?
- **Mindeststandards**
  - „IT-Todsünden“

# Sicherheit durch Innovation



Gesellschaft für  
Freiheitsrechte

## Sicherheit durch Innovationen

- Blockchains statt zentraler Datenbanken
- Tor hidden services statt offener Ports

## tor hidden services

- bisher: Home Automation setzt oft auf „offene Ports“
- Problem: Portscans + unsichere IoT-Geräte
- stattdessen **ek55xbedpam7wn6a.onion** + zufälliger Port



# Beispiele für Mindeststandards

## „Todsünden“ der IT-Security

- Default-Passwörter
- Unverschlüsselte Verbindungen (HTTPS ...)
- fehlende Upgrade-Pfade
- undokumentierte Admin-Backdoors



# Sicherheitslücken als Kosten-Risiko

## Finanzielle Risiken beim Verantwortlichen - Beispiel Produkthaftungsgesetz

- „Hersteller“ ist, wer baut oder vertreibt
- ggf. Regress entlang der Lieferkette
- Regress nicht Problem der Kunden





# Haftung für Sicherheitslücken

## Komplexe Detailfragen

- Open Source
- Haftungsmaßstab?
- Nachweis von Sorgfaltswidrigkeit
- Bezifferung von Schäden im B2C-Bereich – pauschalisierte Schäden?

# Für eine Kultur der IT-Sicherheit



Gesellschaft für  
Freiheitsrechte

Sicherheit muss sich für diejenigen **lohn**,  
die sie in der Hand haben – die Hersteller

- Best Practices / Mindeststandards
  - Wettbewerbsvorteile
  - Haftung



# Auch der Staat muss mitziehen

IT-Sicherheit ist nicht nur  
„nice to have“

Grundrecht auf Integrität und  
Vertraulichkeit informationstechnischer  
Systeme (BVerfG 2008)

„IT-Grundrecht“



# IT-Grundrecht

## Zwei Dimensionen

- Abwehrrecht gegen staatliche Eingriffe
  - Strenge Regeln für „Staatstrojaner“
- Gestaltungsauftrag
  - Das Recht muss sich schützend vor die IT-Sicherheit stellen



# Verfassungsbeschwerde der GFF

## Strafprozessordnung 2017 verfassungswidrig

- Abwehrrecht
  - „Spielregeln“ des BVerfG für Staatstrojaner nicht eingehalten
- Gestaltungsauftrag
  - Wenn der Staat den Einsatz von Lücken erlaubt, muss er hierfür Spielregeln definieren



# Verfassungsbeschwerde der GFF

## Gestaltungsauftrag: Umgang mit Lücken regeln!

- Pflicht zur Meldung unbekannter Lücken
  - Geheimhaltung ist angesichts der möglichen Kollateralschäden unverhältnismäßig
- Nur dem Hersteller bekannte Lücken dürfen ausgenutzt werden
  - Staatstrojaner hat das BVerfG schon erlaubt
  - aber wenn schon, dann „sauber“



Gesellschaft für  
Freiheitsrechte

# Freedom needs Fighters.

[freiheitsrechte.org/join](https://freiheitsrechte.org/join)