Alternativreferat der ÖH Uni Graz
CryptoParty Graz

# Selbstverteidigung im Internet

2.12.2014

# Überblick über den heutigen Abend

- Vorstellung CryptoParty Graz

  **https://cryptoparty.at/graz**


- Einführung in den Themenbereich (Gunter Bauer)
- Email und VPN (Olaf Pichler)
- Sichere Passwörter (Bernhard Zach)
- Der digitale Fingerabdruck/Web-Tracking und Gegenmassnahmen (Anton Kies)

Seit den Aufdeckungen von Edward Snowden wissen wir, dass unsere digitale Kommunikation weltweit von Geheim-diensten überwacht wird.

- Manche wussten / vermuteten das auch schon vorher.
  (vor 25 Jahren: Echelon-System = globales elektronisches Aufklärungssystem)
- Siehe z.B. Erich Moechel, www.fuzo-archiv.at/artikel/1652079v2

# Totalüberwachung

- Warum wird überwacht ?
- Wer überwacht ?
- Wo wird überwacht ?
- Was kann man/frau dagegen tun ?

# Warum Überwachung ?

- Schutz vor Verbrechen und Terrorismus („Krieg gegen Terror“)

- Firmen:
  - Wir wollen den KundInnen maßgeschneiderte, optimierte Produkte anbieten.
  - Deshalb sollten wir die Wünsche der KundInnen genau kennen.
  - Und deshalb sammeln wir
    - Interessensprofile
    - Tätigkeitsprofile
    - Persönlichkeitsprofile

Und:

- Prognosen über zukünftiges Verhalten können gemacht werden

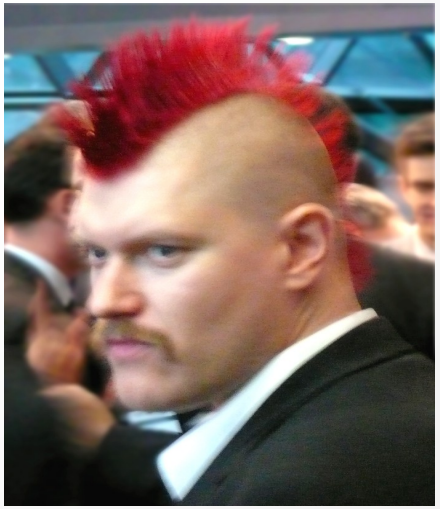
# Wer überwacht ?

- Geheimdienste, staatliche Behörden
- Werbenetzwerke
- Internetkonzerne (amazon, Google, facebook, Apple...)
- Apps-Programmierer

„Kontrollwahn der Konzerne“

(Sascha Lobo,

Schriftsteller, Journalist, Blogger)



# Wer überwacht? (2)

- Kriminelle, die an unsere Kennwörter und Konten heranwollen

- **wir selber**:
  - durch Postings in Sozialen Netzen
  - durch Verwendung von
    - Kreditkarte
    - Kundenkarten
    - Life-Tracker

# Überwachung – was, wo und wie?

- Internet-Surfen, Soziale Netze
- Smartphones
- Smartwatches und Fitness-Armbänder
- Daten in der Cloud:
  - Dropbox, Google Cloud, Evernote, oneDrive, iCloud,...
- Internet of Things:
  - Haushaltsgeräte, Auto, E-Book-Reader, Funkchips, intelligente Stromzähler, Smart City, Fernsehgeräte, ...

# Wo ist das Problem?

Ich habe doch nichts zu verbergen ...

- Doch!

- Jede/r hat ein Recht auf Privatsphäre!
  ( fundamentales Menschenrecht )

# Geschäft mit den persönlichen Daten

- Persönliche Daten sind bares Geld wert

- Daten entscheiden oft mit:
  - wird ein Kredit gegeben?
  - wird eine Leistung der Krankenkassa genehmigt?

→ Aushöhlen der Privatsphäre

# ausserdem …

- Man weiss nicht,
  - wer die Daten hat,
  - an wen sie weitergegeben werden,
  - wie sie verknüpft werden
- Es können falsche Schlüsse gezogen werden

# Was dagegen tun?

**"Digitale Selbstverteidigung"**

- **E-Mails verschlüsseln (→ Vortrag von Olaf)**
- **„Gute“ Passwörter benutzen (→ Vortrag von Bernhard)**
- **Datensparsamkeit: digitale Spur möglichst klein halten (→ Vortrag von Anton)**

# Was dagegen tun? (2)

- Suchmaschinen wechseln
- Web-Browser wechseln
- Anonymisierungs-Tools benutzen
- Cookies entfernen
- Festplatten verschlüsseln
- dezentrale Datenlagerung (wenn möglichst selbst)
- JavaScript einschränken
- Geräte absichern (Updates, Virenschutz, Firewall)
- Wegwerf-Email-Adressen benutzen

# Bildnachweise, Literatur

- ECHELON-Antennenanlage bei Radomes at Menwith Hill, Yorkshire, UK

http://commons.wikimedia.org/wiki/File:Menwith-hill-radomes.jpg

- LUMASCAPE

http://www.heise.de/tp/bild/43/43207/43207_1.html

- Jagd auf die "Kopfjäger" im Internet - Transparenz und Schutz der Privatsphäre im Internet

Artikel von Raúl Rojas 31.10.2014, telepolis

http://www.heise.de/tp/artikel/43/43207/1.html