Crypto Party

Digitale Selbstverteidigung

Wie schützt man sich vor Überwachung?

Geräte im Netz

PIRATEN WÄHLEN

Big Data

Was ist das

- Extrem große Datensammlungen
- Meist dezentral
- Nicht mit normalen Datenbanken zu verarbeiten
- Alle 2 Jahre verdoppeln sich die Daten
- Spezielle Suchalgorithmen
- Ursprünglich im Finanzwesen
- Heute Google/Facebook/NSA/MI5/BND

PIRATEN WÄHLEN

Wer hat die Daten?

- Internet-Provider, Netzbetreiber, Telefongesellschaften
- Alle Dienstanbieter
  - Webseiten
  - Suchmaschinen
  - Mail-Provider
  - Social Media (Facebook, Twitter, Studie-VZ)
- Behörden

Was wird gespeichert

- Handy
  - Standort
  - Kommunikationsdauer / Zeit / Partner
- Computer
  - IP-Adresse
  - Onlinezeit
  - Bestandsdaten
  - Chatprotokolle
  - Bankbewegung

PIRATEN WÄHLEN

Behörden und Daten

- Grundgesetz Artikel 10
  - Briefgeheimnis
  - Preussische Postverordnung 1729
  - Paulskirchenverfassung
  - Bei Bruch schwere Strafen (Körperstrafen/Todesstrafe)
  - Einschränkung nur 1933-1945
  - Deals mit Alliierten (Sondergesetzgebung)
  - Geheimverträge

Behörden
Und Daten

- Daten werden erhoben von privaten Firmen
- Verträge mit Geheimdiensten
- Aushebelung der Grundrechte
- Verfassungsbruch

PIRATEN WÄHLEN

Was macht Überwachung

- Menschen reden nicht mehr offen
- Opposition wird von Regierung überwacht
- Journalisten / Ärzte / Anwälte
- „Ich habe nichts zu verbergen…“
- „…mein Nachbar aber schon“
- Klima des Misstrauens
- Gefahr für Demokratie

PIRATEN WÄHLEN

Was wir Brauchen?

- Völlige Aufklärung
- Whistleblowerschutz
- Starkes EU-Datenschutzrecht
- Intern. Überwachungsabrüstung
- Europäisches PRISM verhindern
- Förderung Datenschutztauglicher Technik„

Grundlagen

Der EMail

- Mails senden
- Mails senden und abholen
- Verschlüsselte Transportwege
- Mails im Zeitalter der Abhörschnittstellen
- Schwachstellen aus Sicht der Vertraulichkeit

Grundlagen

Verschlüsselung

- Symmetrische Verschlüsselung
  - gleicher Schlüssel zum Schließen und Öffnen
- Asymmetrische Verschlüsselung
  - Unterschiedliche Schlüssel
  - Öffentlicher Schlüssel
  - Privater Schlüssel
- In 3-4 Schritten zur verschlüsselten Mail

PIRATEN WÄHLEN

Grundlagen

Verschlüsselung

- **Verarbeitungsstufen (Alice mailt an Bob)**
  - Öffentlichen Schlüssel von Bob besorgen
    - Schlüsselboard im Netz (pgp.mit.edu)
  - Mail mit Bobs öffentlichem Schlüssel verschlüsseln
  - Verschlüsselte Mail mit Alice öffentlichem Schlüssel verschicken
  - Bob entschlüsselt mit seinem privaten Schlüssel

Software!

Aber welche?

- **Betriebssystem**
  - Apple / Chrome OS / Windows
  - Debian / Fedora / Linux
- **Browser**
  - Safari / Chrome / IE / Opera
  - TOR Browser / Firefox / Gnuzilla
- **Suchmaschine**
  - Google / Bing / Yahoo!
  - DuckDuckGo / MetaGer /Startpage

PIRATEN WÄHLEN

Software!

Aber welche?

- **Mailprovider**
  - GMail / Yahoo! Mail / Microsoft Exchange
  - Autistici / MyKolab / posteo / RiseUp / Eigener Mailserver
- **Mail Client**
  - Apple-Mail / Notes / Outlook / Novell Groupwise
  - Thunderbird / Icedove / Enigmail / Claws / Evolution / Kontact
- **Instant Messanger**
  - Google Talk / WhatsApp / Skype / AOL / Viber
  - Pidgin / Adium / Torchat / Xabber

PIRATEN WÄHLEN

Software!

Aber welche?

- **Social Media**
  - Google+ / Facebook / Twitter
  - Buddycloud / Diaspora / Friendica / Lorea / pirati.ca
- **Cloud Storage**
  - iCloud / Dropbox / Skydrive
  - Cozy Cloud / Seafile / ownCloud

PIRATEN WÄHLEN

Verschlüsseln

Was brauch ich?

- **Thunderbird (Mailprogramm)**
- **GPG4win (Verschlüsselungsalgorithmus)**
- **Enigmail (Plugin für Komfort)**
  - Schlüsselgenerierung
  - Schlüsselverwaltung
  - Verschlüsseln
  - Entschlüsseln

PIRATEN WÄHLEN

Wie sieht das praktisch aus?

- Thunderbird runterladen + installieren + konfigurieren
- Ggp4win runterladen + installieren
- Thunderbird starten und Enigmail als Plugin installieren

Vorteile der PGP-Technik

- Web-of-trust
- Dem Schlüssel ein Ablaufdatum geben
- Hybridverfahren → symmetrischer Schlüssel unsymmetrisch geschickt
- Den Schlüssel widerrufen
- Mail signieren

Nachteile der PGP-Technik

- Kein Webmailer mehr
- Neben Bob und Alice gibt es auch Eve
- Absender, Empfänger und Betreff noch immer sichtbar
- Kein vorgelagerter Spam- oder Virenschutz

Fragen und Antworten

- Zeit für Fragen
- Vielen Dank für die Aufmerksamkeit!