Digitale Selbstverteidigung

Meine Daten gehören mir...?

Workshop im Museum für Kommunikation
im Rahmen der Ausstellung „Außer Kontrolle“

22. April 2014 – Rainer Rehak

FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Vorstellung

- Rainer Rehak (Informatik/Philosophie)
- Humboldt Universität zu Berlin
- Lehrstuhl Prof. Wolfgang Coy (Informatik und Gesellschaft)
- Diplomarbeit über heimliche Online-Durchsuchung
- Aktiv im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.
- Aktiv in der Gesellschaft für Informatik e. V.

Hintergrund

- Anstoß: Programm „Echelon“ und jetzt die Enthüllungen von E. Snowden über die globale Überwachung der digitalen Sphäre durch Geheimdienste
  - Gab Material an Journalisten, Inhalt nie bestritten
  - Laut US-Gesetzen kein Whistleblower
  - Gesucht laut Espionage Act (1917) → Geheimgericht
  - Nicht nur NSA, GCHQ: BND liefert aktiv Informationen, steht in regem Austausch und nutzt XKEYSCORE
- „Selbst verschlüsseln“ Ex-Bundesinnenminster Friedrich
  - Analogie: Wasserqualität

Stand der Enthüllungen I

- PRISM, Direktzugriff (Apple (iCloud), Google (gmail, calendar, youtube, gdocs), Facebook, Skype and Microsoft (Office 365)
- Metadaten von Kommunikation, Telefon, Handy, Internet von Providern (Verizon, Orange)
- Direkt am Kabel (Tempura, Upstream), U-Boote
- Google „Intranet“ angezapft
- Exploitdatenbanken für Blackberry, Android, iPhone, Microsoft

Stand der Enthüllungen II

- Aufbau eigener Botnetze (automatisiert)
- Internetinfrastruktur hacken - z. B. den belgischen Provider der EU-Büros Belgacom (über Mitarbeiterlaptops), Blackberrys auf dem G20 in London 2009, UN, SWIFT, HK/China
- Infrastruktur imitieren: Facebook (QuantumInsert), fake-LinkedInseiten, G20-gipfel (2009) falsche Internetcafés

Stand der Enthüllungen III

- Tracking von Personen mit Hilfe von Cookies
- Mobiltelefoninhaltsdaten eines ganzen Landes (nicht veröffentlicht, welches), Merkelaffäre
- Webcams von Millionen Nutzern des Videochat-Dienstes von Yahoo
  - Zu viele Aufnahmen „sexueller Natur"
  - > Filter für Gesichter nötig
- „Zersetzung“ von „Feinden“, z. B. J. Assange

Stand der Enthüllungen IV

- Postpakete abfangen und Geräte verwanzen, Katalog für einzusetzende Bauteile, übermitteln der Daten per Funk
- Verschlüsselungsstandards geschwächt ("Edgehill/Bullrun", Bürgerkrieg)
  - Beeinflussung des NIST bezüglich Schlüssellängen
  - Zusammenarbeit mit Technologiefirmen (Einbau von „Hintertüren“)
  - Verdeckte Agenten in Technologiefirmen einschleusen (SSL-Keys)
- Programm „XKEYSCORE“ führt alles zusammen
- Programm „Boundless Informant“ liefert globale Statistiken

Begründung der Ausspähungen

- "Krieg gegen den Terrorismus"?
  - Zwei voneinander unabhängige Untersuchungs-kommissionen des Weißen Hauses mit Zugang zu den Geheimdokumenten widersprechen der Nützlichkeit
  - Der US-Bundesgerichtshof widerspricht der Nützlichkeit
  - Das White House Privacy and Civil Liberties Oversight Board bewertet das Überwachungsprogramm als komplett ineffektiv: nicht ein einziger Anschlag wurde verhindert, zumal gebe es keine Gesetzesgrundlage

„Nebeneffekte“ der Ausspähungen?

- Überwachung von Institutionen der EU, der UN, der IAEA, das französische Außenministerium, die G8-Gipfel, die G20-Gipfel, COP15 (UN Climate Change Conference in Copenhagen), die deutsche Bundeskanzlerin sowie ihr Kabinett, die türkische und brasilianische Regierung, Südamerikanische Ölfirmen, Visa, Mastercard, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Huawei, Chinesische Führung, US-Anwälte etc.
- USA kannten frühzeitig die Positionen in den Klimaverhandlungen 2009, in Diskussionen über Sanktionen bzgl. des Iran, Positionen der Energie- und Ölpläne südamerikanischer Länder
- Personen mit islamistischem Hintergrund: Konsum erotischer Inhalte gespeichert
- CIA: Überwachung der Computer der Aufklärungsgruppe im Congress
- Wahrscheinlicher Gründe: Privatisierung + Politische Angst
  - z. B. CIA zahlt AT&T jährlich zehn Millionen US-Dollar für Telefondaten
  - Private Contractors profitieren

Workshop „digitale Selbstverteidigung“ I

- Grundsätzlich:
  - Komplexe Welt: Wem vertrauen? (Falschgeld, Nahrungsmittel, Software)
  - Gesellschaftliches Problem
    - Wahl der E-Mailadresse betrifft jeden Kommunikationspartner
    - Steuerdaten über's Internet verschickt
    - Vorratsdatenspeicherung („Nutze kein Internet“)
    - Krankheitsdaten bei Google (UK)
  - Nur freie Software ist perspektivisch sinnvoll

Exkurs: Datenschutz statt Privatheit

- Meine sozialen Daten beim Email-/Telefonanbieter
- Meine Geschäftsdaten bei SAP, Xing, Finanzamt
- Meine Postadressdaten bei Amazon
- Meine Bonität bei meinen Banken
- Meine Krankendaten auf staatlichen Servern
- Meine Dokumente bei Microsoft, Dropbox
- Meine Essgewohnheiten auf der Payback-karte

Es geht also nicht um Privatheit (die jeder anders versteht), sondern

- Schutz der Person und ihrer Entscheidungsfreiheit

Workshop „digitale Selbstverteidigung“ II

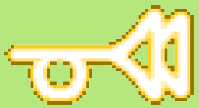
- Nutze Firefox, nicht Safari oder den Internetexplorer (die sind nicht frei, telefonieren nach Hause und sind wenig konfigurierbar)
- Nutze als Suchmaschine: https://startpage.com (anonymisiert Googleanfragen)
- Installiere folgende Firefox-Add-ons:
  - „Self-Destructing Cookies" (über Extras→Add-ons, Cookies werden gelöscht, wenn man die jeweilige Seite verlässt)
  - „Adblock Edge" (über Extras→Add-ons, Werbeblocker ohne Ausnahmen)
  - „HTTPS-Everywhere" (immer auf die verschlüsselte Version von Webseiten umleiten) https://www.eff.org/https-everywhere
  - „discnnect.me". Blockiert aktive Trackingelemente auf Webseiten (Socialnetworks, Werbung) https://disconnect.me/
  - Tor-Browser-Bundle (ein modifizierter Firefox inklusive aller nötigen Add-ons, der über das Anonymisierungsnetzwerk Tor läuft) https://www.torproject.org/download/download-easy.html
- Android: Nutze TextSecure, statt Whatsapp/Threema/Telegram/usw. TextSecure ist freie, und damit diskutierbare Software

Workshop „digitale Selbstverteidigung“ III

- Nutze kleinere Mailprovider, die eine Haltung haben, z.B. uberspace.de, so36.net oder riseup.net
- Nutze Emailverschlüsselung: OpenPGP oder S/MIME (z.B. mit dem Emailclient Thunderbird und dem Add-on Enigmail) 0D66 63E5 70A3 964A EE60 D927 4427 CFE5 8C19 AE19
- Installiere das Firefox-Add-on "RequestPolicy" (über Extras → Add-ons, verhindert, dass externe Inhalte von Webseiten geladen werden)
- Installiere das Firefox-Add-on "NoScript" (über Extras → Add-ons, verhindert, dass Scripte auf Seiten ausgeführt werden)

Nächste Veranstaltungen / Links

- Museum für Kommunikation: 17. Mai 20 bis 0 Uhr „Lange Nacht der Museen“
- Beckmann „Informiert oder manipuliert – wie die digitale Welt unser Leben verändert“, ARD: http://www.daserste.de/unterhaltung/talk/beckmann/sendung/17042014-informiert-oder-manipuliert-100.html
- Nochmal die Tipps aus dem Workshop (und mehr): http://berlin.fiff.de/workshop2204.html
- „Warum wir Google fürchten“, Döpfner, FAZ http://www.faz.net/aktuell/feuilleton/medien/mathias-doepfner-warum-wir-google-fuerchten-12897463.html?printPagedArticle=true#pageIndex_2



Danke