„Wir waren zu naiv“

Wie die Entwicklung von Echelon bis Prism zeigt, wird eine ahnungslose, globale Zivilgesellschaft seit 30 Jahren militärisch angegriffen. Legistische Maßnahmen dagegen allein genügen nicht. Zuerst müssen die Kommunikationsnetze der Zivilgesellschaft so gehärtet werden, dass die Kosten für Angriffe auf diese Daten in lichte Höhen steigen.

erich@moechel.com Europäischer Datenschutztag 2014 01 28

Die Nebel von Echelon

- 1947 UKUSA Vertrag => Funkspionage, Kabel
- 1973 UK und NO erste europäische Knoten des ARPAnet, "packet switched" wie TCP/IP.
- "Echelon" = Truppenformation zum Angriff über die Flanke. Schlacht von Leuktra 371 A.D.
- 1983 Reagans "Star Wars" Abwehrraketen im TV, real Satellitenspionagenetz ausgebaut: Verbund mit bestehendem System
- E-Mail Protokoll standardisiert [John Postel]

Die Geburt eines Monsters

- 1988 Digitalisierung dringt in Firmen und Privatsphäre ein. Sowjetimperium bricht zusammen.
- Handlungsbedarf bei der NSA. Die zivile Vernetzung wächst der Kontrolle davon.
- Die Privatisierungswelle unter Reagan wird auf den Geheimdienstkomplex ausgeweitet.
- Private Public Partnerships.
- 1992 Premiere: NSA-Direktor William Studemann wechselt in die Privatwirtschaft.

Ein Präsident der CIA

- 1988 Mit George H.W. Bush wird der erste CIA-Direktor US-Präsident.
- 1993 Quantico VA: 'FBI' Briefing für EU-Polizei und Partnerdienste
- Überwachung des digitalen Mobilfunks. Fokus: Analyse von Metadaten.
- 1995 CALEA Gesetz für Überwachungs-Interfaces im Mobilfunk.
- EU: Ratsbeschluss im Fischereiausschuss zur Mobilfunk-Überwachung

Echelon fliegt auf, Crypto Wars

- NSA blockiert sichere Verschlüsselung in Webbrowsern – Pläne für "Clipper Chip"
- GCHQ fordert "key escrow" für Krypto = Vorab-Hinterlegung der Schlüssel
- 1996 Nicky Hager [NZ] dokumentiert und verortet das globale Echelon-System.
- NSA kontrolliert Domain Name Service des WWW auch weiterhin global.
- Immer mehr Medienberichte über Echelon

Bis zur Jahrtausendwende

- 1996 NSA-Direktor Mike McConnell wechselt zum Contractor Booz Allen Hamilton
- 1997 "Lawful Interception" Standards für Mobil funk im ETSI, GCHQ leitet Arbeitsgruppe.
- Schadsoftware: Aus Viren werden Würmer
- 2000 Echelon U-Ausschuss im Europarl.
- NSA verliert Crypto Wars, Verschlüsselung wird für Export nach und nach freigegeben
- Basiskomponenten für sichere Kommunikation bereits vorhanden: PGP, SSL, HTTPS

"War on Terror" – "Patriot Act"

- 2001 Ministerium für Heimatschutz, US "Intelligence Community" wächst explosiv
- Glasfasernetze, SWIFT Finanzdaten, Passenger Name Records.
- 2006 SWIFT Skandal fliegt auf. EU beauftragt Booz Allen Hamilton mit "Sicherheitsaudits".
- Medien: NSA kopiert Verkehr in Glasfaser-netzen von AT&T, Verizon. 10 Gbit Switches
- Gesetz verleiht US-Carriern Immunität. Erste Sammelklagen werden abgewiesen.

Was Snowden miterlebte

- 2005 Keith Alexander neuer NSA-Direktor
- 2007 Donald Rumsfeld holt McConnell als Obersten Koordinator der Geheimdienste
- 2010 Alexander fällt Cyber Command zu
- 2009 Amtsantritt Obamas, McConnell wechselt wieder zu Booz Allen.
- Black Budget" des Geheimdienstkomplexes überschreitet 50 Milliarden Dollar
- Zwei Millionen US Bürger mit "Top Secret"

Post Snowden - Lagebericht

- Die NSA kann keine guten Schlüssel knacken
- Angriffsvektoren sind daher Implementation, Peripherie und Betriebsysteme.
- Herstellerbedingte Sicherheitslücken werden nicht gemeldet sondern ausgenützt.
- Das macht die zivilen Netze für Angriffe von Cyberkriminellen extrem verwundbar.
- NSA & Co nutzen Cyberkriminelle als Nebelwerfer, infiltrieren deren Schadsoftware.

Parva Strategica

- NSA-Überwachungsansatz: Naive Nutzer, US-Betriebsysteme, US-Cloudservices
- 30 Jahre konnten die US-Dienste ihre Systeme ungestört zum Moloch ausbauen.
- Die NSA läuft auf Linux, nur "Open Source"-Systeme lassen sich überprüfbar absichern
- Schon einfache Sicherheitsmaßnahmen steigern Komplexität und Kosten jedes Angriffs.
- End-to-End-Crypto zwischen Mailservern, Datencenters und auf Carrierebene

Support the NSA going dark

- Alles => HTTPS, TLS, SFTP usw.
- Darunter: PGP/GnuPG für Mail, Jabber/OTR für Chat. Neue Kryptoanwendungen vor Launch.
- Schon einfache Gegenmaßnahmen verlangen durchwegs komplexe Konter der NSA.
- Nur in diesem Rahmen sind politische und legistische Maßnahmen wirkungsvoll
- **Die bestehenden NSA-Systeme skalieren unter solcher Belastung nichtlinear negativ**

PGP KEY 0x2440DE65

http//:fm4.ORF.at/erichmoechel

pgp key **0x2440DE65**

fingerprint

A564 1457 71C3 E907 6D78 429E 76F3 C66E 2440 DE65

OTR signature, https upload

https://moechel.com

harkank@jabber.ccc.de @harkank

erich@moechel.com

Berlin, Datenschutztag 2014 01 28