Problemskizzierung

Informationskrieg und -frieden

Spannungsfelder und Entspannungswege

in elektronischen Netzen

Andy Müller-Maguhn

andy@ccc.de

Sprecher, Chaos Computer Club e.V.

Infowar Symposium

Bundesnachrichtendienst / Pullach 02. November 2000

Zum Chaos Computer Club

- Geschichte, Aufgabe und Funktion
  - 1981 Treff von Computerfreaks, die sich für elektronische Kommunikationsnetze interessierten
  - seit 1984 Herausgabe der Zeitschrift Datenschleuder und Veranstaltung des jährlichen Chaos Communication Congress
  - 1986 Gründung des Chaos Computer Club e.V. als Konsequenz des 2. WiKG (Regelung von Verantwortlichkeiten)
- Vereinsziele
  - Einsatz für ein Menschenrecht auf zumindest weltweite ungehinderte Kommunikation
  - Förderung von Informationsfreiheit und Transparenz (z.B. maschinenlesbare Regierung)
  - Auseinandersetzung mit gesellschaftlichen Folgen von Technologie (Chancen, [Rest-]risiken, Nebenwirkungen)
- Praktische Arbyte / Organisationsform
  - Bundesweiter Verein, organisiert in Dezentralen, Erfa-Kreisen und Chaos-Treffs
  - Betrieb von Kommunikationsstrukturen und Medien (Datenschleuder, Web- & Listserver, CD-ROMs)
  - Durchführung & Teilnahme von/an Veranstaltungen (Congress & Camp, Workshops, Anhörungen, Sonstige)

Die Hackerethik*

- **Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert,**
  sollte unbegrenzt und vollständig sein.
- **Alle Informationen müssen frei sein.**
- **Misstraue Autoritäten - fördere Dezentralisierung.**
- **Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien**
  wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- **Man kann mit einem Computer Kunst und Schönheit schaffen.**
- **Computer können dein Leben zum Besseren verändern.**
- ***Mülle nicht in den Daten anderer Leute.***
- ***Öffentliche Daten nützen, private Daten schützen.***

---

* vorläufige Arbeitsversion & Diskussionslage. Siehe auch
https://www.ccc.de/Hackerethik.html

Angriffskategorien & Motivationen

- Hacker
  - Neugier, Förderung von Informationsfreiheit & Transparenz
- Cracker
  - Befreihung eingesperrter Bits (Kopierschutzmechanismen)
- Crasher
  - Vandalismus/Kaputtwillspaß als Frust-Ableiter (LOVE-LETTER-FOR-YOU)
- Kriminelle
  - materielle Interessiertheit (Geld)
- Spione
  - Zugang und Verfälschung von Information
- Soldaten (Infowar)
  - Zerstörung/Manipulation/Zersetzung elektronischer Infrastruktur

Infowar Entwicklung & Hackerszene

- 1987: VAX/VMS V. 4.4/4.5
  "Ereignisse um eine Betriebssystemfehler", Stefan Weirauch
- 1988: KGB / Karl Koch
  Auswirkungen auf Hackerszene und die Beteiligten
- 1989: BSI / IFIS (Pohl)
  Öffentliche Strukturierung "ehemaliger" Nachrichtendienststrukturen
- 1995: Infowar-Diskussion (Schwartau)
  Versuch der "Nutzung" von Hackern zur Szenarien-Demonstration
- 1998: Rekrutierungen, Anwerbungen
  Auswirkungen auf Beteiligte und die Entwicklung
- 1999: LOU Angriffsmobilisierung & Abwehr
  Nichtangriffspakt der Hackerszene

Problemlage & Bedrohungsszenarien

- Technische Grundlagen und Struktur des Internet
  - Protokollschwächen TCP/IP v4 ermöglichen Sniffing, Spoofing, Denial of Service etc.
  - Netzarchitektur (DNS) als single point of failure konstruiert; unter Kontrolle des USG
  - Netz- & "Sicherheits-"strukturelemente (Router, Firewalls etc.) oft Blackboxen (SBO) mit eingebauten Trapdoors
  - Sicherheit auf Clientseite aufgrund Marketing- & Monopolstrategie stark unterentwickelt
- Politische Einschränkungen der Sicherheit (auf Netz- und Sicherheitsproduktebene)
  - Bestehende Auswirkungen von Export-Restriktionen auf Verschlüsselungs- und Sicherheitsprodukte
  - "Sicherheitsprodukte" schaffen oft zentrale Kontrolloptionen und begünstigen Mißbrauchsszenarien
  - SIGINT - Strukturen á la Echelon; Begünstigungen von SIGINT durch ETSI-Methode der "Lawful-Interception"
  - Politisch motivierte Modellversuche zur Erzeugung mangelhaft untermauerten Bewusstseins (DDOS/NIPC)

Sicherheits- und Unsicherheitspolitik

- Sanktionierung von Computerstraftaten
  - "klassische" Computergesetzgebung (BRD: 2. WiKg, 1986)
  - Verbot von aktiven Angriffen (Eindringen, Ausspähen, Verändern etc.)
- US / G8 / COE Vorstoss "Cyber Crime Convention"
    - Verbot von Angriffswerkzeugen = Einschränkung von Überprüfungsoptionen
    - Ausweitung von staatlichen Überwachungsbefugnissen = Schaffung zusätzlichen Mißbrauchspotentials
- Repräsentative Wahrnehmung von IT-Sicherheitspolitik
  - im Ergebniss sinnfrei bzw. kontraproduktiv
- Entwicklung eigener Strategien stark ausbaufähig
  - strukturelle und technologische Unabhängigkeit

Empfehlungen

- Rahmenbedingungen
  - Freiheit von Verschlüsselungstechnik, Reeingeneering, Angriffs- und Abwehrinstrumenten
  - Haftungsregulierung im Anwendungsbereich definieren (Verantwortung des Betreibers)
- Technische Aufgaben
  - Dezentrale Strukturen fördern zur Vermeidung der "single point of failure"
  - Proaktive Formulierung von Anforderungen für kritische IT-Bereiche
- Aktive Maßnahmen
  - Förderung von Open-Source Technik und transparenten Strukturen
  - Aufdeckung von Sicherheitsprobleme und Behebung aktiv fördern

Weitere Informationen

https://www.ccc.de

mail@ccc.de

(Wir sind kein Dienstleister. Wir machen nur öffentliche Arbeit.)