Computer-Unsicherheit aktuell

Handlungsstränge und Optionen

Andy Müller-Maguhn

andy@ccc.de

Sprecher, Chaos Computer Club e.V.

Expertengespräch der CDU/CSU Bundestagsfraktion, Berlin 11.09.2000

Zum Chaos Computer Club

- Geschichte, Aufgabe und Funktion
  - 1981 Treff von Computerfreaks
  - seit 1984 Herausgabe 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 zmd. weltweite ungehinderte Kommunikation
  - Förderung von Informationsfreiheit und Transparenz (z.B. maschinenlesbare Regierung)
  - Auseinandersetzung mit gesellschaftlichen Folgen von Technologie (Restrisiken, Nebenwirkungen, Chancen)
- 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*

- **Die 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 Dezentralierung.**
- **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

Akteure und Motivationen

- Hacker
  - Neugier, Förderung von Informationsfreiheit & Transparenz
- Cracker
  - Befreiung eingesperrter Bits (Kopierschutzmechanismen)
- Crasher
  - Vandalismus/Kaputtwillspaß als Frust-Ableiter ("I HATE TO GO TO SCHOOL")
- Kriminelle
  - materielle Interessiertheit (Geld)
- Spione
  - Zugang und Verfälschung von Information
- Soldaten (Infowar)
  - Zerstörung/Manipulation/Zersetzung elektronischer Infrastruktur

Eckpunkte der Entwicklung

- 1986 / 87 NASA-Hack
  - Hintergrund: Sicherheitsloch in VAX/VMS 4.4 / 4.5
  - präventive Information an BfV / Pohl, Veröffentlichung durch Bekanntwerden des Hacks in SPAN/NASA
- 1988 / 89 KGB-Story
  - technischer Hintergrund de fakto gleich; Koch und weiterer Kronzeuge stellen sich Mitte 1988, Urteile Mitte 1989
  - Tod von Karl Koch während seiner Aussagen und unter Führung des VS im Frühjahr 1989
- 1994 / 95 Supporting
  - Mißbrauch des Telekom-Netzes zum Gelddrucken
  - Risiko-Entwicklung und juristische Abfederung bei Einführung neuer Technologien vernachlässigt
- 1997 / 98 Versuch der Kryptoregulierung in Deutschland
  - Besuch des US-Sonderbotschafters Aaron bei BK Kohl und BMI Kanther; Kanther-Rede BSI Congress April 97
  - Weitere Aktivitäten von Aaron und transatlantisches Engagement
- 1998 BND-Anwerbewerbeversuch in der Szene & Tod des Berliner Hackers Tron
  - zunehmende wirtschaftliche und politisch/strategische Bedeutung vernetzter Computer
  - Tod des Hackers Tron im Spannungsfeld von organisierter Legalität, Kriminalität und ausländischen Diensten
- 1999 MS-Crypto API etc.
  - Abhängigkeit der Bundesregierung von sicherheitseingeschränkter Technologie durch US-Export Richtlinien
  - BSI stimmt erstmals der Notwendigkeit von Open-Source Technologien für Regierungsaufgaben zu
- 2000 Technische Vorfälle mit politischen Fragen
  - DDOS-Attacken und das NIPC-Budget, I-LOVE-YOU Virus und die G8-Cybercrime Convention
  - MPAA vs. 2600 Prozess wg. DeCSS und Folgen

Aktuelle Situation & Aktivitäten

- 18.10.1999 - Sitzung des EU-Rats für Justiz und Inneres zur Strategie ENFOPOL -> ETSI
  The Commission, whilst noting that its position has not changed, informed delegations that a possible way to break the deadlock could be following a similar strategy as that followed in tackling the issue of Child Pornography in the Internet. Although acknowledging that this was a different topic it also has an interception dimension.
- 01.02.2000 - Anhörung im US-Senat / Budget-Verhandlung NIPC
  WASHINGTON, Feb 1 (Reuters) - A White House plan to protect telecommunications, energy and other key systems from cyberattacks relies too much on detecting intrusions and not enough on improving security, a report by Congress' investigative arm said on Tuesday.
- 10.02.2000 - DDOS-Attacken (u.a. CNN, YAHOO etc.)
  Gezielte Ausnutzung unsicherer Computersysteme als Angrifssplattform auf Medienunternehmen etc.
- 16.02.2000 - Bewilligung im US-Senat
  "Everything hacked but the budget." (Declan McCullagh in Wired)
- 28.03.2000 - EU - Rechtshilfeabkommen von Luxemburg blockiert
- 12.04.2000 - Sitzung des BSI im BMI der Task Force "Internet Sicherheit"
  Teilnahme einer amerikanischen Delegation von 4 (!) Mitarbeitern
- 27.04.2000 - Entwurf Cyber Crime Convention wird offiziell veröffentlicht
- 04.05.2000 - "ILOVEYOU" - Virus (VBS) verbreitet sich auf MS-Outlook Systemen
- 15.05.2000 - G8 HTC Sitzung in Paris (Diskussion der Cyber Crime Convention)

Entwurf d. "cyber crime convention"

- **Verfügbar: "declassified public version". Eckpunkte (Auszüge):**
- Größter teil: klassische Gesetzgebung, die in Deutschland bereits seit 1986 (!) besteht:
  - § 1 Definition § 2 Access § 3 Interception § 4 Data Interference § 5 System Interference
  - § 7 Computer related forgery § 8 Computer related fraud
- Fachlich unsinniges Verbot von "Angriffswerkzeugen / Fernwartungs- und Überprüfungswerkzeugen"
  - § 6 kontraproduktive Einschränkung der überprüfbaren und überprüften Sicherheit
  - Adaption von Innenminister Schily
- § 9 Offenses related to child pornography; § 10 Copyright offenses
- § 17 Traffic data; § 18 Interception
  - "under discussion"
- § 27 Transboarder Access; § 28 Interception

  "under discussion"

Ziele und Zielkonflikte

- Sicherheit
  - Restrisikohandling
- Überwachung
  - wirft eigene Sicherheitsprobleme auf (Datenschutz, Akzeptanz, Sicherung der anfallendern Daten und Überwachungsschnittstellen)
- "Gesetzmässiges abhören"
  - "Deregulierung der Telekommunikation", Diskussion um den TKG §90 etc.
- Einschränkung von Sicherheitsmaßnahmen
  - Kryptoregulierung, Verbot von Werkzeugen etc.
- Wünschenswert: vorbildliche Strukturen auf Regierungsebene
  - Transparenz (inkl. Risiko-Benennung); offene Schnittstellen (Interoperabilität)
  - Einsatz von beherrschbarer Technologie und Kompetenzförderung
- Notwendig: Risiko-Regulierung durch gesetzliche Rahmenbedingungen
  - Beweislastumkehr- bzw. Schadensbegrenzungsmechanismen

Weitere Informationen

https://www.ccc.de

mail@ccc.de