Exploit Regulations

AT-Cyber-Sonderedition

fukami <fukami@ccc.de> • Metalab, Wien • 21. Oktober 2013

$ whois fukami

- IT-Sicherheitsberater (SektionEins GmbH)
- Mitgliedschaften: u.a. Digitale Gesellschaft e.V., CCC e.V., Open Data Network e.V., Liquid Democracy e.V., seit kurzen CCC-Vertreter bei EDRi
- Politischer Schwerpunkt: Technik und deren Einfluss auf Gesellschaft


SORRY NO PICS!

Cyber Cyber!

Was ist dieses Cyber von dem sie alle reden

- bedeutet ursprünglich **Steuerung**
  Kybernetike „Kunst des Steuermanns“
- 1948 erstmal im Bereich Datenverarbeitung genutzt
  siehe Norbert Wiener: Kybernetik – Regelung und Nachrichtenübertragung in Lebewesen und Maschinen / Cybernetics or control and communication in the animal and the machine
- vorwiegend kulturelle und technik-philosophische Nutzung z.B. Cyberpunk, Cyberkultur, Cybernaut, Cyberspace, Cyborg etc.

Was ist dieses Cyber von dem sie alle reden

- ***Cyber*** ist Markenname von Control Data Corporation (Computer in den 70ern und 80ern)
- Legislativ existiert der Begriff/die Vorsilbe in Deutschland nicht
- Nationales Cyber-Abwehrzentrum -> unsinnig
  “Cybersecurity” ergibt zumindest *etwas* Sinn
- IN AT: Cyber Crime Competence Center (C4)
- Heute im allgemeinen Sprachgebrauch eher negativ konnotiert, z.B. Cyberterrorismus, Cyberkrieg

IT-Sicherheit in the real world

IT-Sicherheit ist

- stark markt- und innovationsgetrieben
- Forschung: konkrete Lücken, neue Klassen
  Stichwort: Vulnerability Development
- ein riesiger Markt: Exploit-Verkauf, Consulting, Sicherheitslösungen
- ein weites Feld: von Social Engineering über Targeted Attacks bis Massenexploitation
- voller Fragen mit unklaren Antworten, z.B. “Wem gehört eine Sicherheitslücke?” (dem Entwickler, dem Finder der Lücke, dem Käufer einer Lücke usw.)

Zur Verteidigung gehören

- Incident-Response
- Herstellung von Integrität, Vertraulichkeit und Anonymität
- Abwehr gegen direkte Angriffe auf Infrastruktur (z.B. DDoS, Einbrüche, Defacements)
- Abwehr gegen Massenexploits und Targeted Attacks
- Analyse von Angriffen, Schadcode, Filtersystemen
- Prävention, Datenschutz
- Folgenminderung und Wiederherstellung
- Verkleinerung der Angriffsoberfläche

Für IT-Sicherheit Verantwortliche auf staatlicher Seite in DE

- liegt prinzipiell im Inneren
  - BMI, BSI
  - Polizei: BKA und LKAs
    dazu: BKA KI 2/TESIT: Technisches Entwicklungs- und Servicezentrum, Innovative Technologien
  - IT-Planungsrat und Untergruppen, Arbeitsgruppen der Länder und Kommunen
    Kontext: IT-Interoperabilitäts- und IT-Sicherheitsstandards
  - Nationales Cyber-Abwehrzentrum (NCAZ)
    Im Kern: BSI, BfV, BBK dazu BKA, BND, Bundespolizei, Bundeswehr und Zollkriminalamt
  - Datenschutzbeaftragte des Bundes und der Länder

Mit IT-Sicherheit befasste zivilrechtliche und privatwirtschaftliche Gruppen

- Vielzahl von Akteuren: OS-Hersteller, Vendor, Sicherheits-Unternehmen, kleine Beratungsfirmen, freie Sicherheitsexperten
- Hacker und Hacktivisten, z.B. CCC, cDc
- 31337 DE/AT (z.B. 7350/teso, Phenoelit, THC)
- Deutscher Sonderweg: Reverse Engineering ist prinzipiell erstmal nicht verboten (in den USA: DMCA)

Gesetzliche Regelungen

Grundgesetzliche Regelungen und Schranken (DE)

- “Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”
  auch IT-Grundrecht, Computer-Grundrecht oder Grundrecht auf digitale Intimsphäre
- Zeugnis- und Auskunftsverweigerungsrecht
- Prinzipielle Einschränkungen invasiver Zugriffe:
  - tatsächliche Anhaltspunkte
  - konkrete Gefahr
  - überragend wichtiges Rechtsgut betroffen

Gesetzgebung in DE: Computerstraftaten

- Ausspähen von Daten gemäß § 202a StGB
- Vorbereiten des Ausspähens und Abfangens von Daten gemäß § 202c StGB
- Computerbetrug § 263 a StGB
- Datenveränderung gemäß § 303a StGB
- Computersabotage gemäß § 303b StGB
- Fälschung beweiserheblicher Daten §§ 269/270 StGB
- Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen gemäß § 108b UrhG

Gesetzgebung in AT: Computerstraftaten

- Widerrechtlicher Zugriff auf ein Computersystem § 118a StGB
- Verletzung des Telekommunikationsgeheimnisses § 119 StGB
- Missbräuchliches Abfangen von Daten § 119a StGB
- Datenbeschädigung § 126a StGB
- Störung der Funktionsfähigkeit eines Computersystems § 126b StGB
- Missbrauch von Computerprogrammen oder Zugangsdaten § 126c StGB
- Betrügerischer Datenverarbeitungsmissbrauch § 148a StGB

Welche Straftaten werden mit Hilfe der Nutzung des Internets begangen? (DE)

- Verbreitung pornografischer Schriften gemäß § 184 ff. StGB
- Volksverhetzung und Gewaltdarstellung gemäß §§ 130, 131 StGB
- Betrug gemäß § 263 StGB
- Unerlaubte Veranstaltung eines Glücksspiels gemäß § 284 StGB
- Urheberrechtsverstösse gemäß §§ 106 bis 108a UrhG

Welche Straftaten werden mit Hilfe der Nutzung des Internets begangen? (DE)

- Strafnormen im Markengesetz
  gemäß §§ 143 ff MarkenG
- Strafnormen im Wettbewerbsrecht (UWG)
  strafbare Werbung §§ 16 ff. UWG
- Strafnormen im Datenschutzgesetz (BDSG)
  Bußgeld nach § 43 und § 44 BDSG (unbefugte Datenerhebung)

Computer-Gesetze sonstwo (Grobauswahl)

- EU: **Budapest Convention on Cybercrime**
- US: **CFAA** (Computer Fraud and Abuse Act), **DMCA** (Digital Millenium Copyright Act)
- UK: **Computer Misuse Act**, **Police and Justice Act**
- Irland: **Criminal Damage Act, Criminal Justice (Theft and Fraud Offences) Act, Data Protection Acts**

Sonstige Regelungen

- Telekommunikationsgesetz (in DE **TKG**): Datenschutz, Wettbewerbsregeln/Marktregulierung, Abhören von Nachrichten, Anmeldepflichten, VDS/BDA, Manuelles Auskunftsverfahren, Verbraucherschutz, (Sperren)
- Telemediengesetz, Medienregulierung auf Länderebene
- Frequenzverwaltung
- ITU, ISO-Normen
- Datenschutzgesetze, Signaturgesetze, Informationsfreiheits-/Transparenzgesetze
- DE-Mail-Gesetz

“The Tallinn Manual”

- NATO-Treffen in Tallinn
- Cyberwar-Doktrin
- US-Vertreter: *Wenn jemand Sicherheitsprobleme veröffentlicht, die US-Infrastruktur betreffen, so kann die USA diese Person zu einem Kriegsziel erklären.*

Exportregulierung für Überwachungstechnik

- Reporter ohne Grenzen, Digitale Gesellschaft, CCC, Privacy International, ...
- Vor drei Jahren praktisch alternativlos, aber nun *eventuell* eine Gefahr
- Fokus:
  - Schmutzige/fragwürdige Geschäftsmodelle (z.B. Gamma Group)
  - Infection Proxies, Angriffswerkzeuge gegen Dissidenten
- Problem: Die Definition von “Digitalen Waffen”

Ein bisschen Theorie

Worüber reden wir?
Universalmaschinen

- **Computer sind universelle Maschinen, die programmierbare Vorschriften verarbeiten.**
- Aber: Nicht alles lässt sich in entsprechende Vorschriften pressen. Es gibt theoretische und praktische Grenzen.

Die universelle Maschine: Grundlegende Modelle

- Die ***Turingmaschine*** ist ein mathematisches Konzept zur formalen Definition eines Begriffes der ***Berechenbarkeit***.
- Die ***Von-Neumann-Architektur*** (VNA) ist ein ***Referenzmodell für Computer***, wonach ein gemeinsamer Speicher sowohl Computerprogrammbefehle als auch Daten hält.

Die universelle Maschine: Grundsätzliche, formale Probleme

- ergeben sich u.a bei der ***Software-Verifikation***, *z.B.*:
  - Halteproblem (auch: Problem der Unentscheidbarkeit)
  - Gödelscher Unvollständigkeitssatz

Die universelle Maschine: Turings Halteproblem

- Erreichen formale Systeme einen bestimmten Grad an Komplexität, so kann über deren Zustand nichts mehr ausgesagt werden.
- ***In jeder Turingmaschine lassen sich Aussagen formulieren, die weder bewiesen noch widerlegt werden können.***

Die universelle Maschine: Erster Unvollständigkeitssatz

- Der Erste Unvollständigkeitssatz besagt, dass es in hinreichend starken widerspruchsfreien Systemen immer unbeweisbare Aussagen gibt.
- ***Jedes hinreichend mächtige formale System ist entweder widersprüchlich oder unvollständig.***

Die universelle Maschine: Zweiter Unvollständigkeitssatz

- Der Zweite Unvollständigkeitssatz besagt, dass hinreichend starke widerspruchsfreie Systeme ihre eigene Widerspruchsfreiheit nicht beweisen können.
- ***Jedes hinreichend mächtige konsistente formale System kann die eigene Konsistenz nicht beweisen.***

Was sind Exploits?

- Mehrfachbedeutung: Gefundene Lücke, aber auch Code, der diese ausnutzt
- In unbeweisbaren Systemen kann es zu Zuständen kommen, die nicht mit Annahmen übereinstimmen
- Unintended/Unwanted/Unauthorized Code Execution
  Evil Computation

  Must Read: “Avoiding a War on Unauthorized Computation: Why Exploit Regulation is the Biggest Danger to Coder Freedom and Future Security” - Paper von Sergey Bratus und Anna Shubina (Dartmouth)

Was wir brauchen

Welche Fragen sind wichtig?

- Was braucht die Zivilgesellschaft um technische (sprich: reale) Sicherheit herzustellen?
- Wo beisst sich das mit der militärischen Sicht/die Sicht der Geheimdienste auf kritische Infrastruktur?
- Helfen z.B. Geheimdienste, kritische Infrastruktur sicherer zu machen?

Was wir brauchen

- Generell:
  - Eine von Technik abhängige Gesellschaft muss jederzeit in der Lage sein, Soft- und Hardware zu prüfen und Probleme zu fixen
  - Das generelle Recht, Unsicherheit zu thematisieren
  - Fail FTW: Ordentliche Fehlerkultur

Was wir brauchen

- Konkret:
  - Bessere Gewährleistung: Keine Sanktionen für Bugs, aber für nicht gefixte Sicherheitslücken
  - Sanktionen anhand Motivation und Schaden ausrichten; klarere Schwellen definieren
  - Kein Vendor-only Disclosure
  - Verbot für Geheimdienste, Backdoors in öffentlicher Infrastruktur oder per Order in kommerzieller Software zu hinterlegen, bewusst Crypto oder Standards zu schwächen
  - Source Escrow(?)

Danke für die Aufmerksamkeit!