Einführung in das deutsche und europäische Computer- und Internetstrafrecht

Dr. Alexander Koch
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Gang des Vortrags

- Relevante Taten.
- Deutsches Computer- und Internetstrafrecht.
- Europäisches Computer- und Internetstrafrecht.

Relevante Taten

- „Klassisches Hacken“ - Einbrechen in fremde Rechner:
  - Passives Ausspionieren von Systemen (ping, Portscann etc.),
  - aktives Ausspionieren von Systemen (Testen von Schwachstellen),
  - Einbrechen in fremde Systeme,
  - „Stehlen“ von Daten,
  - Vernichten von Daten,
  - illegale Nutzung,
  - Verwischen von Spuren.

Relevante Taten

- (D)DoS-Angriffe.
- Viren, Würmer & Trojaner sowie Botnetze.
- Phishing:
  - Aufstellen der Falle,
  - Nutzen der Daten.
- Dialer:
  - Installation der Dialer,
  - Zahlungsforderung.

Relevante Taten

- ***Nicht*** behandelt werden:
  - Urheberrechtsdelikte,
  - Pornographie,
  - Hassdelikte,
  - sonstige Delikte, die lediglich das Internet als neues Medium nutzen.

„Epochen“ des deutschen Computer- und Internetstrafrechts

- Klassisches Strafrecht (19. und 20. Jh.),
- Maschinenstrafrecht (ab 1935),
- frühes Computerstrafrecht (1986),
- aktuelles Internetstrafrecht (2007).

„Klassisches“ Strafrecht

- Betrug:
  - Problem: Ein Mensch muss irren; nicht anwendbar, wenn eine Maschine „irrt“.
  - Aber: Dialer-Kriminalität konnte erfasst werden!
- Sachbeschädigung:
  - Würde die „virtuelle“ Zerstörung erfassen: Ein Computer mit gelöschtem Betriebssystem ist ein unbrauchbarer Computer.
- Fazit: Strafrecht war auf körperliche Gegenstände und handelnde Menschen zugeschnitten.

„Maschinenstrafrecht“ (1935 / 69)

- Erschleichen von Leistungen (1935):
  - Erfasst wurde schon früh das „illegale“ Telefonieren.
  - Phreaking (Cap’n Crunch).
  - Geschützt werden aber nur „öffentliche Telefonnetze“, nicht erfasst ist also die Verwendung eines fremden (eroberten) Rechners.
- Fälschung technischer Aufzeichnungen (1969):
  - Zugeschnitten auf mechanische Aufzeichnung.
  - Eine „abtrennbare“ Aufzeichnung wird verlangt – Logfiles werden also nicht erfasst (andere Sichtweise aber durchaus möglich!).

„Maschinenstrafrecht“

- Fazit: Das Strafrecht hat sich der Technisierung früh angepasst und Maschinenleistungen / -produkte erfasst.

„Frühes Computerstrafrecht“ (1986)

- Ausspähen von Daten a.F. („Datendiebstahl“):
  - Überwinden eines Zugangsschutzes erforderlich.
    - Nicht erfasst wird etwa das Pingen oder passive „Ausspähen“ von Sicherheitslücken.
    - Keine hohen Anforderungen an den Zugangsschutz (auch schlechte Passwörter).
  - Daten mussten „verschafft“ werden.
    - Jedes „Ansehen“ von Daten über ein Netz setzt ein Verschaffen voraus.
  - Erfasst wird der „Datendiebstahl“ durch Hacker oder Schadprogramme.
  - Nicht strafbar war der bloße „Einbruch“ in ein System (aber bereits der erste Blick ...).

„Frühes Computerstrafrecht“

- Fälschung beweiserheblicher Daten:
  - Fälschung „hypothetischer“ elektronischer Urkunden. Geschützt werden nur menschliche Gedankenerklärungen – etwa elektronisch gespeicherte Verträge, aber auch E-Mails.
  - Bislang keine besondere praktische Bedeutung.
  - Aber: Spam und Phishing mit gefälschten Absenderkennungen lassen sich erfassen.

„Frühes Computerstrafrecht“

- Datenveränderung („virtuelle“ Sachbeschädigung):
  - Der „echten“ Sachbeschädigung nachgebildet.
  - Erfasst wird „Vandalismus“ auf gehackten Systemen;
  - aber auch Veränderungen / Manipulationen durch Viren, Würmer & Trojaner.

„Frühes Computerstrafrecht“

- Datenveränderung (Fortsetzung):
  - Dialer („klassischer“ Betrug durch Versenden der Rechnungen).
    - Aber: In der Praxis in erster Linie ein zivilrechtliches Problem.
      - Die Rechtsprechung hat in der Praxis geholfen und Zahlungsansprüche verneint.
      - Telekommunikationsrechtliche Gesetzgebung: Registrierpflicht für Dialer, spezielle Nummerngassen.
      - 2005: 21.559 Beschwerden bei der Bundesnetzagentur.
      - 2007 (1. HJ): 26 Beschwerden bei der Bundesnetzagentur.
  - Das Problem ist zivil- und verwaltungsrechtlich gelöst worden, nicht strafrechtlich!

„Frühes Computerstrafrecht“

- Computersabotage a.F.:
  - „Besonders schlimme“ Datenveränderung; erfasst wurden nur die Computer von „Betrieben“ und „Unternehmen“ – nicht aber private Systeme.
  - (D)DoS-Angriffe.
- Computerbetrug:
  - Auch Computer können durch Täuschung zu einem „Irrtum“ verleitet werden.
  - Verwendung von Kontodaten beim Phishing.
    - Für den Finanzagenten auch Geldwäsche.

„Frühes Computerstrafrecht“

- Fazit:
  - Der Gesetzgeber hat auf die Computerkriminalität der 80iger-Jahre reagiert.
  - Nur der „böse“ Hacker sollte strafbar sein, nicht aber der Schüler, der sich aus technischer Neugier in ein fremdes System hackt.
  - Das Computerstrafrecht aus dem Jahre 1986 war in der Lage, völlig neue Erscheinungsformen der Computerkriminalität wie Phishing und (D)DoS-Angriffe zu erfassen.
  - Es bedarf also nicht bei jeder neu aufkommenden Technik neuer Tatbestände.

„Neues Internetstrafrecht“ (2007)

- Ausspähen von Daten n.F. („virtueller Hausfriedensbruch“):
  - Es müssen keine Daten mehr „verschafft“ werden.
- Abfangen von Daten:
  - Sniffing, TEMPEST (diskrete Abstrahlung).
- Computersabotage n.F.
  - Auch private Systeme „von wesentlicher Bedeutung“ werden erfasst.

„Neues Internetstrafrecht“

- Vorbereiten des Ausspähens und Abfangens von Daten („Hackerparagraph“):
  - Programmieren und Verbreiten von „Hackerwerkzeugen“.
  - Gesetzgeberische Intention: Vertrieb von Viren, Würmern & Trojanern sowie Angriffssoftware sollte unterbunden werden.
  - Problem: Dual-use-Software: Schwachstellenscanner kann eingesetzt werden, um in ein fremdes System einzubrechen oder um das eigene System zu prüfen.
  - Grenzen noch völlig offen.

„Neues Internetstrafrecht“

- Fazit:
  - Es gibt kein „sportliches“ Hacken mehr.
  - Praktisch alle Verhaltensweisen, die über ein „Betrachten“ fremder Systeme von „außen“ hinausgehen, sind strafbar.
  - Möglicherweise sogar Überkriminalisierung; jedenfalls starke Verunsicherung in der „guten“ Sicherheitsszene.

Europäisches Computer- und Internetstrafrecht

- Übereinkommen über Computerkriminalität des Europarates (Cybercrime Convention).
- Rahmenbeschluss über Angriffe auf Informationssysteme der EU.

Cybercrime Convention

- Von Serbien (und Montenegro) am 7.4.2005 unterzeichnet, aber noch nicht in Kraft gesetzt.
- Von der Bundesrepublik ebenfalls unterzeichnet, aber noch nicht in Kraft gesetzt, wohl aber in weiten Teilen schon umgesetzt.

Cybercrime Convention

- Katalog von Taten, die strafbar sein müssen:
  - Rechtswidriger Zugang,
  - rechtswidriges Abfangen,
  - Eingriff in Daten („Sachbeschädigung“),
  - Eingriff in ein System („Behindern des Betriebs“),
  - Missbrauch von Vorrichtungen („Hackertools“),
  - computerbezogene Fälschung / Betrug,
  - Kinderpornographie,
  - Urheberrechtsverletzungen.

Cybercrime Convention

- Formen der Verantwortlichkeit:
  - Täterschaft, Beihilfe und Anstiftung,
  - Versuch,
  - juristische Personen („Unternehmensstrafrecht“).
- Weitere Regelungen:
  - Regelung ermittlungstechnischer Mindestmöglichkeiten (Abhören, Beschlagnahme),
  - internationale Zusammenarbeit.

Rahmenbeschluss über Angriffe auf Informationssysteme

- ***WICHTIG:*** EU, nicht EG! Es handelt sich nicht um supranationales Recht, sondern um „einfaches“ Völkerrecht.
- „Cyberterrorismus“.
- Katalog von Taten, die strafbar sein müssen:
  - Rechtswidriger Zugang zu Informationssystemen,
  - rechtswidriger Systemeingriff,
  - rechtswidriger Eingriff in Daten.

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

IRNIK
Dr. Alexander Koch
Postfach 15 01 61
53040 Bonn
DEUTSCHLAND
Tel.: +49-2 28-8 50 86 63
Fax: +49-2 28-8 50 86 62
ak@irnik.de
http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie