Verband der deutschen Internetwirtschaft e. V.

Rechtliche Aspekte beim Kampf gegen Botnetze

Frank Ackermann
Senior Legal Counsel, eco

Agenda

- **Rechtliche Maßnahmen gegen Botnetz-Betreiber und Botnet-Spammer**
- **Datenschutz beim Aufspüren eines Zombies im Kundennetz**
- **Eindringen in Botnetze und ihre Infrastruktur (Dropzones und Zombie-Rechner)**
- **Schwierigkeiten polizeilicher Ermittlungen gegen Botnetzbetreiber**
- **Szenario: Der regelwütige Gesetzgeber**
- **Update: eco Anti Spam Initiative zur Botnet-Strategie von eco/BKA und BSI**

Rechtliche Maßnahmen gegen Botnetz-Betreiber und Botnet-Spammer

Das scharfe Schwert: Strafrecht

- **Datenveränderung (§ 303a StGB) „virtuelle Sachbeschädigung“**
- **Computersabotage (§ 303b StGB), häufig besonders schwerer Fall, gewerbsmäßig - Störung einer Datenverarbeitungsanlage durch eine Datenveränderung nach § 303a StGB (DoS)**
- **Fälschung technischer Aufzeichnungen (§ 268 StGB) - Logdaten**
- **Ausspähen von Daten (§ 202a StGB) „elektronischer Hausfriedensbruch“, also auch bloßes Entern strafbar**
- **Abfangen von Daten (§ 202b StGB) - etwa Keylogging**
- **Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) - gilt auch für § 303b StGB**

Rechtliche Maßnahmen gegen Botnetz-Betreiber und Botnet-Spammer

Zivilgehorsam: Der Unterlassungsanspruch nach dem BGB

- **§ 1004 (ggf. analog) i.V.m. § 823 BGB – verschuldensunabhängig**

Fair Play: Wettbewerbsrecht

- **Unzumutbare Belästigung (§ 7 UWG)**
- **Unlautere geschäftliche Handlung (§ 3 UWG)**
- **Gewinnabschöpfung (§ 10 UWG)**
- **USA: “Herbal King”**

Kehren vor der eigenen Haustüre: die AGB

Datenschutz beim Aufspüren eines Zombies im Kundennetz

Beispiel: BotHunter

analysiert passiv Datenverkehr

sammelt alle relevanten Informationen

Bericht enthält Angaben zu den beteiligten Rechnern sowie auch Kopien der Malware, die der verseuchte Rechner herunter geladen hat.

Datenschutz beim Aufspüren eines Zombies im Kundennetz

Spannungsverhältnis ?

§ 202b StGB Abfangen von Daten

-

§ 88 TKG Fernmeldegeheimnis

Datenschutz beim Aufspüren eines Zombies im Kundennetz

§ 202b StGB

Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendungvon technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Datenschutz beim Aufspüren eines Zombies im Kundennetz

§ 88 TKG

Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist

Datenschutz beim Aufspüren eines Zombies im Kundennetz

jedoch

§ 88 TKG

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste ***einschließlich des Schutzes ihrer technischen Systeme*** erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, ***nur für den in Satz 1 genannten Zweck verwenden.***

Datenschutz beim Aufspüren eines Zombies im Kundennetz

Vorherige Gestattung durch Verfügungsberechtigten (-) unklar, wessen Daten abgefangen werden

Genehmigung (nachträgliche Erlaubnis) (-) im Strafrecht

Bisher keine Rechtsprechung zum Verhältnis § 202b StGB und § 88 Abs. 3 Satz 1 TKG

Bestrafung der nach TKG erlaubten Sicherungsmaßnahmen wäre systemwidrig.

§ 202b StGB geht auf Umsetzung des Art. 6 Abs. 1 Cybercrime-Convention zurück.

Art. 6 Abs. 2 Cybercrime Convention: „Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise **zum genehmigten Testen oder zum Schutz eines Computersystems** erfolgt. „

Eindringen in Botnetze und ihre Infrastruktur (Dropzones und Zombie-Rechner)

Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Urteil des BVerfG vom 27.02.2008 - 1 BvR 370/07, 595/07)

Glashaus: § 202c StGB ?

Verteidiger erfüllt die gleichen Techniken und TB wie Angreifer. Unterschied: Rechtfertigungsebene

Eindringen in Botnetze und ihre Infrastruktur (Dropzones und Zombie-Rechner)

Notwehr- / Notstandsfähige Rechtsgüter

Jedes rechtlich geschützte Interesse des Verteidigers oder bei Nothilfe des Opfers.

– also auch: „virtuelles Hausrecht“

Notwehr

- **Geeignetheit**
- **Erforderlichkeit (Gebotenheit) - das mildeste geeignete Mittel**

Notstand

- **Geeignetheit**
- **Erforderlichkeit**
- **Güterabwägung (Angemessenheit) Rangfolge der Rechtsgüter, Grad der drohenden Schädigung**

Gilt NICHT für den White Hat Hacker - dessen Handeln bleibt strafbar

Eindringen in Botnetze und ihre Infrastruktur (Dropzones und Zombie-Rechner)

Staatliches Handeln ?

Gesetzesvorbehalt

- **Jedes belastende staatliche Verhalten bedarf einer ausdrückliche Ermächtigungsgrundlage.**

Bestimmtheitsgebot

- **Gesetze müssen so bestimmt sein, dass der Bürger klar erkennen kann, was ihn erwartet.**

Verhältnismäßigkeitsgrundsatz

- **Jedes staatliche Handeln muss verhältnismäßig sein.**

Besonderheiten polizeilicher Ermittlungen gegen Botnetzbetreiber

Internationale Dimension

Zügige Informationsbeschaffung bei ISPs erforderlich, insb. bei Gefahr im Verzug

Hase & Igel

Erleichterung durch dezentrale Steuerung ?

Szenario: Der regelwütige Gesetzgeber

Chancen für ein Gesetz, das das Fernmeldegeheimnis auf den Kopf stellt und Provider verpflichtet, Spam zu unterdrücken?

Szenario: Der regelwütige Gesetzgeber

Chancen für ein Gesetz, das das Fernmeldegeheimnis auf den Kopf stellt und Provider verpflichtet, Spam zu unterdrücken?

- **Schlechte Erfolgsaussichten haben den Gesetzgeber bisher nicht von Regelungen abgehalten - siehe etwa § 6 TMG.**

Szenario: Der regelwütige Gesetzgeber

Chancen für ein Gesetz, das das Fernmeldegeheimnis auf den Kopf stellt und Provider verpflichtet, Spam zu unterdrücken?

- **Schlechte Erfolgsaussichten haben den Gesetzgeber bisher nicht von Regelungen abgehalten - siehe etwa § 6 TMG.**
- **Politischer Mehrwert fraglich - ISPs haben eigenes Interesse, mit Augenmaß zu filtern**

Szenario: Der regelwütige Gesetzgeber

Chancen für ein Gesetz, das das Fernmeldegeheimnis auf den Kopf stellt und Provider verpflichtet, Spam zu unterdrücken?

- **Schlechte Erfolgsaussichten haben den Gesetzgeber bisher nicht von Regelungen abgehalten - siehe etwa § 6 TMG.**
- **Politischer Mehrwert fraglich - ISPs haben eigenes Interesse, mit Augenmaß zu filtern**
- **Durchsetzbarkeit fraglich - Ham ? Spam ?**

eco Anti Spam Initiative zur Botnet-Strategie von eco/BKA und BSI

Botnet-Problematik wird im FB Content des eco behandelt

BSI/eco haben ersten Botnet-”Workshop” am 29.10.2008 in Wiesbaden organisiert

Ab sofort: Runder Tisch

Nächster Termin: 25.02.2009

Treffen ISPs/BKA/LKÄ geplant für April 2009

Verband der deutschen Internetwirtschaft e. V.

Ihre Fragen ?

eco
RA Frank Ackermann
Lichtstr. 43 h
50825 Köln
Tel.: 0221 / 70 00 48 – 240
Fax: 0221 / 70 00 48 – 111
E-Mail: frank.ackermann@eco.de
Web: http://www.eco.de