Spam

Geißel der Menschheit?

Peter Koch
Internet Society German Chapter e.V.
pk@ISOC.DE

2005-02-04

Visite

- Anamnese und Diagnose
- Epidemie
- Hysterie
- Prophylaxe und Hygiene
- Wunderheiler und Scharlatane
- Pharmaka I
- Kontraindikationen
- Pharmaka II
- Prognose

Spam: Wo wir stehen

- Unerwünschte (Massen-)Mail
- Belastet die Empfänger
- . . . vermeintliche Versender
- . . . Provider (`abuse`)
- . . . die technische Infrastruktur
- Unerwünscht, aber trotzdem vorhanden
- Nutzbarkeit des Mediums wird eingeschränkt
- Spezielle Medienkompetenz ist gefragt

Wie verbreitet ist das Problem?

- Subjektive Wahrnehmung: ∞
- Studien: 30 - 100+% aller Mails sind Spam
- n% allen Spams kommt aus *XX*, *YY* und *ZZ*
- ISPs nutzen Zahlen blockierter(!) Mails als Werbeargument
- Regierungen und Regulierer sind aufmerksam
- . . . und fühlen sich zu Reaktionen verpflichtet/ermuntert

Das Ende des Netzes ist nah . . .

News at Eleven:

- „E-Mail ist nicht mehr nutzbar!“
- „100.000.000 EUR/USD/. . . Schaden monatlich/jährlich!“
- „Das Mailprotokoll ist vollkommen untauglich!“

Quis custodiet ipsos custodes?

Erste, leichte Gegenmaßnahmen

- Protokollkonformität erzwingen ($\leadsto$ Spammer lernen schnell(er))
- Schwarze Listen (offener Relays, DialUp-Bereiche, . . .)
- *Subscriber Only* Mailinglisten
- *Double Opt-In* Mailinglisten
- Vorsicht bei der Preisgabe der eigenen Adresse

Wunderheiler und Scharlatane

- Einfach klingende Lösungen sind nicht immer geeignet
- Vernon Schryvers Liste zur
  Final Ultimate Solution to the Spam Problem
  `http://www.rhyolite.com/anti-spam/you-might-be.html`
- Die E-Mail-Infrastruktur ist ein komplexer Mechanismus

Technische Gegenmaßnahmen . . .

- Schwarze Listen – bekannte(?) Spam-Quellen
- *Greylisting* – initialer Malus mit Whitelist-Option
- *Sender Callout* – Online-Prüfung der Absenderadresse
- Opt-In – Mailannahme nach Tokenübermittlung
- Filter – Schlüsselworte, Bayes
- Prüfsummensammlung – *DCC*
- Portblocks – keine direkt ausgehende Mail
- . . .

. . . und ihre Nebenwirkungen

- Schwarze Listen – werden instrumentalisiert/juristisch angegriffen
- *Greylisting* – Skalierungsprobleme
- *sender callout* – dto., auch: Wechselwirkungen
- Opt-In – Akzeptanz, Skalierung, Einsetzbarkeit
- Prüfsummen – Datenschutz, Fernmeldegeheimnis
- . . .

Filter

- . . . schießen über ihr Ziel hinaus (*Rechtsexpertin*)
- Lernende Filter
  - *State of the Art*
  - erfolgreich, wenn benutzersteuerbar
  - werden vergiftet: Text vs. HTML, oben Viagra – unten Goethe

Was tun mit erkanntem Spam?

- Je nach Behandlung Eingriff in das Post- und Fernmeldegeheimnis
- Extremansichten: §206 StGB Unterdrückung
- Wer liest und versteht Fehlermeldungen?

Technische Maßnahmen auf Protokollebene

- IETF-Arbeitsgruppe *MTA Authorization Records in the DNS*
- RMX, SPF, MAIL From: SenderID, Domain Keys, BATV, CSV, ...
- Problem: Insellösungen, Fragmentierung
- Problem: Patente, Egos, Marketing und Beratungsresistenz
- MARID ist tot,
  MASS (Message Authentication Signature Standards) lebt

IETF – gescheitert?

+ keine technische Lösung standardisiert
– keine *schlechte* technische Lösung standardisiert
– Prozeß nicht instrumentalisiert
– technische Arbeit geht weiter

Vielleicht hilft verbieten?

- §1004 BGB (DE)
  - Abschreckung offensichtlich gering
- §7 UWG (DE) – *Unzumutbare Belästigung*
  - Stumpfes Schwert für Verbraucher
- Gesetzentwurf *Anti-Spam-Gesetz* ($\rightsquigarrow$ TDG)
  - Einführung eines OWi-Tatbestandes
  - Verschleierung des Absenders oder der *kommerziellen Natur*
  - `Subject: ADV: Tags sind Unfug`?
  - Internationale Wirkung?

Wie geht es weiter?

- Komplexe Anti-Spam-Systeme können Kleinanwender ausgrenzen
- Peering-Beziehungen zwischen Providern (*später Sieg für X.400* :-) oder Insellösungen
- Nebenwirkungen sind störend und werden es noch eine Weile sein
- Viren, Würmer, Phishing

Also ist Spam eine Geißel der Menschheit?

- Ja, aber eine von Menschen gemachte
- Spam ist ein soziales Problem, daß nicht nur technisch bekämpft werden kann
- E-Mail wird weiter existieren
- Das *Ende-zu-Ende-Prinzip* wird (weiter) leiden
- Technische Maßnahmen werden Quellen- oder Proxy-Authentisierung einschließen sowie Bewertungssysteme
- Technische Maßnahmen müssen durch Sanktionen flankiert werden
- . . . werden neue Angriffsvektoren erschließen (z.B. DNS)

Gefahren der Überdosierung

- Technische Komplexität
- Zentralisierung
- Silbernes Tablett für *Bedarfsträger* (TKÜV)