SPAM – Was kann man als Einrichtung im DFN dagegen tun?

Ralf Hildebrandt
Charité Campus Mitte
ralf.hildebrandt@charite.de

27. März 2002

Zusammenfassung

Spam, UCE, UBE: Welche Maßnahmen gegen "Spam" sind sinnvoll, welche nicht?

Ansätze zur Bekämpfung von Spam

Spam kann auf drei Arten geblockt werden. . .

- anhand inhaltlicher Kriterien:
  - Header
  - Body
- anhand syntaktischer bzw. technischer Kriterien:
  - syntaktische Fehler
  - Protokollfehler
- anhand schwarzer Listen
  - RBL-style Blacklists
  - RHSBL-style Blacklists

Begutachtung des Inhalts

Dies kann aufgrund §10[1] Grundgesetz problematisch sein.

Allerdings ist gerade ein Scan auf Viren sicherlich im Sinne des Benutzers, sodaß hierbei von einem impliziten Einverständnis ausgegangen werden kann.

Problematischer sind dabei allerdings das Abweisen von Emails mit dubiosen Headern wie z.B. diesen `Subject:` Zeilen:

- `MAKE MONEY FAST`
- `Enlarge your Penis`
- `Want to be a millionaire?`
- usw.

Denn evtl. **wünscht** der Benutzer den Empfang solcher Emails (siehe z.B. Institut für Sexualkunde).

[1] Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Filterung anhand technischer Kriterien

Glücklicherweise stellen die einschlägigen RFCs[2] genügend Anforderungen an das SMTP Protokoll, die von zahlreichen "Spamwares" nicht erfüllt werden.

Als Betreiber kann man also immer argumentieren, daß die Mail

- angenommen würde, sobald sie protokollkonform eingeliefert wird
- abgewiesen wurde, da sie **im Fehlerfalle** nicht hätte gebounced werden können.

Auf der nächsten Folie sind einige technische Kriterien sowie ihre Realisierung in der Konfiguration von `Postfix` dokumentiert. Die Konfigurationsoptionen für Exim und Sendmail sind ganz ähnlich.

[2] RFC 821, RFC 2821

Einige technische Kriterien

Zu diesen technischen Kriterien gehören:

- HELO/EHLO erforderlich:
  `smtpd_helo_required = yes`
- strikte Einhaltung der Syntax für Envelope Sender und Recipient:
  `strict_rfc821_envelopes = yes`
- Voll-qualifizierte Envelope Sender und Recipient Adressen:
  `reject_non_fqdn_sender, reject_non_fqdn_recipient`
- Offensichtlich nicht-existente Absenderdomainen:
  `reject_unknown_sender_domain, reject_unknown_recipient_domain`
- Pipeliningversuche **vor** Bekanntgabe der Pipeliningfähigkeit:
  `reject_unauth_pipelining`
- ungültige Hostnamen im HELO/EHLO Argument:
  `reject_invalid_hostname`
- nicht voll-qualifizierter Hostname im HELO/EHLO Argument:
  `reject_non_fqdn_hostname`

Filterung anhand "Schwarzer Listen"

Es gibt zahlreiche "schwarze Listen" (blacklists), die man einsetzen kann:

- RBL-style
  Hierbei wird die IP der Gegenstelle in der Blacklist gesucht
  - `www.mail-abuse.org`
    kommerziell
  - `www.ordb.org`
    zuverlässig, automatisiert, international
  - `socks.relays.osirusoft.com`
    blockt offene Proxies
  - `rblmap.tu-berlin.de`
- RHSBL[3]-style
  Hierbei wird der Domainenanteil (alles hinter dem @) in der Blacklist gesucht.
  - `www.rfc-ignorant.org`
    Listet Domains, die:
    * keinen `postmaster` oder `abuse` Account haben[4]
    * keine Bounces annehmen[5].

[3] right hand side black list
[4] RFC 2142
[5] RFC 2821

Probleme bei “Blacklists”

Bei Einsatz von Blacklists treten ab und zu Probleme auf:

- Mailserver von Korrespondenten sind gelistet
  Häufigkeit: Tritt selten auf
  Lösung: Administrator kontaktieren
  Workaround: Ausnahme definieren

- zuviele DNS Lookups
  Häufigkeit: Tritt immer auf
  Lösung: Caching DNS

- DNS Server der Blacklist ist nicht erreichbar
  Häufigkeit: Tritt selten auf
  Lösung: Caching DNS

Konsequenz:
Ein **dedizierter** Caching DNS Server ist ein gute Idee.
`http://cr.yp.to/djbdns.html` hat keine Sicherheitslücken und ist um Größenordnungen schneller als BIND.

Prüfung der Header

Spamware erzeugt oft Header, anhand derer man sie erkennen kann:

```
# Weise Mails mit 4 non-printable Zeichen zurueck
/[^[:print:]]{4}/       REJECT Headers must not contain unprintable characters

# Spam mit Subject: Blahfasel     565876
/^Subject:.*[[:space:].]{5,}\(?#?[[:digit:]]{2,}\)?$/   REJECT Spam

/\r/    REJECT Lone CR in headers indicates virus or spam!
# Zur Begruendung:
# http://online.securityfocus.com/archive/1/257287
```

Virenscanner

Virenscanner funktionieren nicht[6].

Wenn man sie dennoch einsetzen muß, um den Meltdown des Netzes zu verhindern, bleiben folgende Anforderungen:

- schnell; besser: schneller
- automatische, inkrementelle Updates
- läuft nicht mit Superuser-Privilegien
- hat keinen Zugriff auf das gesamte Dateisystem

Problem:

- kein "professioneller" Virenscanner bietet alle diese Features

Lösung:

- Einsatz von "unprofessioneller" (lies: Open Source) Software: `avcheck` oder `amavis`.

[6] Turingsches Halteproblem

Ausblick

Ein Ausblick auf die Zukunft von Spam und Viren:

- "Spammer" werden besser
  Spam läßt sich nicht mehr von legitimer Mail unterscheiden.
- Viren werden Virenscanner angreifen
  Virenscanner sind ein lohnendes Ziel, da sie mit Systemprivilegien laufen und an zentraler Stelle eingesetzt werden.
- DoS durch Virenscanner
  Schon jetzt können "professionelle" Systeme durch einfachste Mittel in ihrer Arbeit unterbrochen werden.

Diskussion

Er hat “Jehova” gesagt.