Blocklisten

Agenda

- Was sind Blocklisten
- schwarze oder weiße Listen
- lokale oder entferne Listen
- Anwendung mit Postfix
- fertige Listen
- Zusammenfassung

Was sind Blocklisten?

- Listen mit:
  - E-Mail Adressen
  - IP-Adressen
  - IP-Blöcken (Dail-Up)
  - Domainnamen

Schwarz oder Weiß?

- Whitelist/Positivliste
  - IP/Empfänger/Absender/... wird bevorzugt
  - Vertrauen in Absender/Empfänger/...
  - Probleme beim Absender
- Blacklist/Negativliste
  - IP/Empfänger/Absender/... wird benachteiligt
  - ablehnen/löschen/kennzeichnen

Lokal oder Entfernt?

- lokale Listen
  - Hash/Access-Map

```
abuse@abwesend.com        OK
@alteDomain               REJECT
```

  - PCRE

```
/^Subject: SAVE GERMANY VOTE STOIBER.*/ REJECT
```

Lokal oder Entfernt?

- entfernte Listen (DNS-Blocklisten)
  - Datenschutz?
  - Missbrauch (http://www.heise.de/newsticker/meldung/91417/)
  - wenig Systemressourcen, DNS-Queries verhältnismäßig billig
  - Beispiel Spamhaus
    - SBL - bekannte Spammer
    - XBL - gekaperte Rechner
    - PBL - „Non-MTA IP address ranges“

lokale Listen in Postfix

- check_helo_access

  ```
  mail.abwesend.com                    550  Das bin ich!
  ```

- check_recipient_access

  ```
  @alteDomain                          REJECT
  ```

- check_sender_access

  ```
  abwesend.com                         OK
  ```

- check_client_access

  ```
  192.168                              REJECT
  ```

- body_checks

  ```
  /Hot Horny Girls/                    OK
  ```

- header_checks

  ```
  /^Subject: SAVE GERMANY VOTE STOIBER.*/     REJECT
  ```

entfernte Listen in Postfix

- Check für 82.198.69.144

```
host 144.60.198.82.pbl.spamhaus.org

144.60.198.82.pbl.spamhaus.org has address 127.0.0.11
```

- reject_rbl_client

```
reject_rbl_client sbl.spamhaus.org

reject_rbl_client xbl.spamhaus.org

reject_rbl_client zen.spamhaus.org

reject_rbl_client dnsbl.sorbs.net

reject_rbl_client list.dsbl.org
```

fertige Listen

- Malware Blocklist (http://www.malware.com.br)
  - PCRE-Liste auf Malware spezialisiert
- Spamhaus.org
  - DNS-Blacklist
- Distributed Checksum Clearinghouse - DCC
  - fuzzy Prüfsummen über Spammails
- Pyzor
  - Hash über Spammails

Zusammenfassung

- vor dem Einsatz prüfen!
- lokale Listen
    - mehr Pflegeaufwand
    - weniger Effektiv
    - kein Kontrollverlust
- entfernte Listen
    - effektiver

Vielen Dank für die Aufmerksamkeit

Fragen?