Nolisting

„Wir stellen uns einfach tot“

Agenda

- Was ist Nolisting
- Nolisting und RFC
- Nolisting einrichten
- Was bringt Nolisting?
- Zusammenfassung

Was ist Nolisting?

- „Normal“
  - absichtlich toter primary MX
  - 10/20 Setup
- Modifikation
  - Sandwich-MX 10/20/30 (tot/lebend/tot)

Geht das mit rechten Dingen zu?

- RFC 2821 konform!
  - „To provide reliable mail transmission, the SMTP client MUST be able to try (and retry) each of the relevant addresses in this list in order, until a delivery attempt succeeds. However, there MAY also be a configurable limit on the number of alternate addresses that can be tried. In any case, the SMTP client SHOULD try at least two addresses.“

Was brauch ich dazu?

- MX-Einträge erstellen

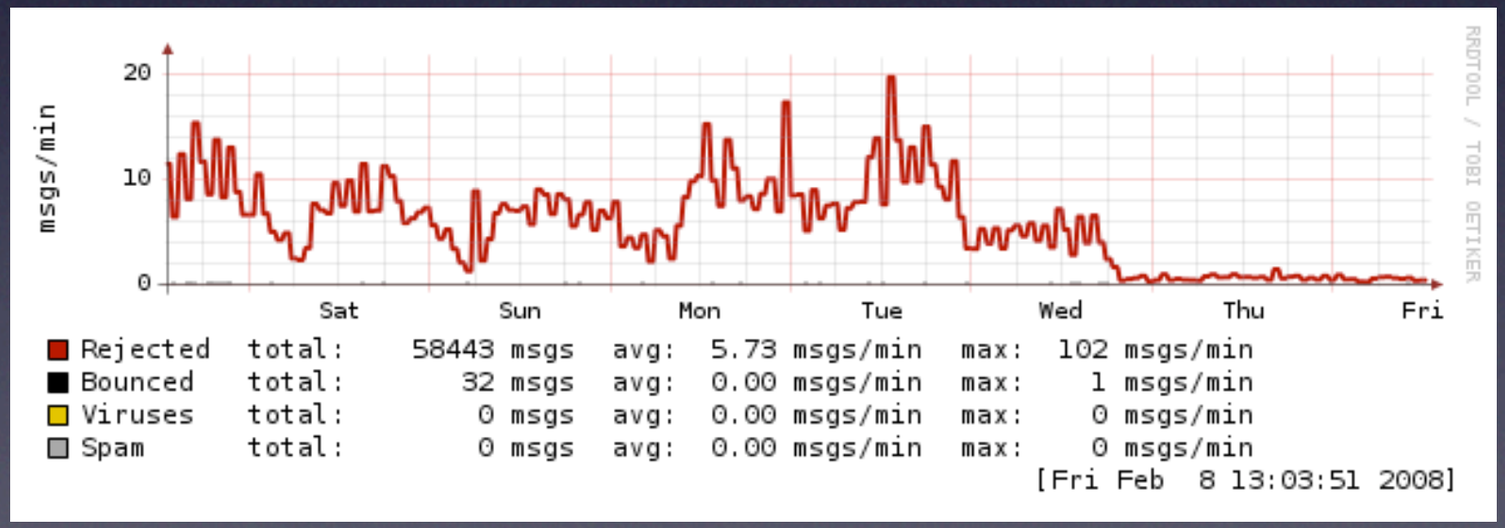
```
MX      10      fakemx.abwesend.com
MX      20      mail.abwesend.com
```

- öffentliche IP && Paketfilter

```
iptables -I INPUT -p tcp -d $IP --dport 25 \
-j REJECT --reject-with tcp-reset
```

Wozu das ganze?

- 90% weniger Spam zu prüfen
  - keine SMTP-Verbindungen
  - keine Inhaltsanalyse



Wo ist der Trick?

- Spammer nicht RFC konform
- Dank tcp-reset keine spührbare Verzögerung

Beispiel

```
20:53:55 pickup:   7C3227C02CE: uid=1002 from=<ben>
20:53:55 cleanup:  7C3227C02CE: message-id=<20080327195355.7C3227C02CE@farbsucht.de>
20:53:55 qmgr:     7C3227C02CE: from=<ben@farbsucht.de>, size=314, nrcpt=1 (queue active)
20:53:58 smtpd:    connect from localhost[127.0.0.1]
20:53:58 smtpd:    369ED7C007E: client=localhost[127.0.0.1]
20:53:58 cleanup:  369ED7C007E: message-id=<20080327195355.7C3227C02CE@farbsucht.de>

20:53:58 qmgr:     369ED7C007E: from=<ben@farbsucht.de>, size=739, nrcpt=1 (queue active)

20:53:58 smtpd:    disconnect from localhost[127.0.0.1]
-------------------------------------------------------------------------------------------
20:53:58 smtp:     7C3227C02CE: to=<ich@abwesend.com>, relay=127.0.0.1[127.0.0.1]:10024, delay=2.8,
                   delays=0.04/0/0/2.8, dsn=2.6.0, status=sent (250 2.6.0 Ok, id=29325-05,
                   from MTA([127.0.0.1]: 10025): 250 2.0.0 Ok: queued as 369ED7C007E)

20:53:58 qmgr:     7C3227C02CE: removed

20:53:58 smtp:     connect to fakemx.abwesend.com[85.131.209.11]: Connection refused (port 25)

20:53:58 smtp:     369ED7C007E: to=<ich@abwesend.com>, relay=mail.abwesend.com[85.131.209.8]:25, delay=0.13,
                   delays=0.06/0/0.04/0.03, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as DD550128285)

20:53:58 qmgr:     369ED7C007E: removed
```

Zusammenfassung

- vor dem Einsatz prüfen!
- RFC 2821 konform
- schnell eingerichtet
- sehr wirksam gegen Fire&Forget-Spam
- erhebliche Entlastung bei Bot-Angriffen
- wirksam gegen Exchange-Admins ;)
- http://nolisting.org/

Vielen Dank für die Aufmerksamkeit

Fragen?