

Inhalt

Filter am Mailserver

SpamAssassin und CRM114

PDFs

Rejects vs. Bounces

- Wichtigste „Verteidigungslinie“
- E-Mail sofort ablehnen (Reject)
 - quasi kein Ressourceneinsatz
 - keine Inhaltsprüfung
 - keine Verantwortung und Bounces
- nach Weiterleitung schon verloren

ilpostino.jpberlin.de



MX für uplug.de:
mail.variomedie.de



Listenserver:
mail.asta.uni-potsdam.de

Rejects vs. Bounces

- Wichtigste „Verteidigungslinie“
- E-Mail sofort ablehnen (Reject)
 - quasi kein Ressourceneinsatz
 - keine Inhaltsprüfung
 - keine Verantwortung und Bounces
- nach Weiterleitung schon verloren

ilpostino.jpberlin.de



pD9E2FC4C.dip.t-dialin.net



MX für uplug.de:
mail.variomedie.de



Listenserver:
mail.asta.uni-potsdam.de

Rejects vs. Bounces

- Wichtigste „Verteidigungslinie“
- E-Mail sofort ablehnen (Reject)
 - quasi kein Ressourceneinsatz
 - keine Inhaltsprüfung
 - keine Verantwortung und Bounces
- nach Weiterleitung schon verloren

ilpostino.jpberlin.de



pD9E2FC4C.dip.t-dialin.net



MX für uplug.de:
mail.variomedia.de



REJECT

Listenserver:
mail.asta.uni-potsdam.de

Rejects vs. Bounces

- Wichtigste „Verteidigungslinie“
- E-Mail sofort ablehnen (Reject)
 - quasi kein Ressourceneinsatz
 - keine Inhaltsprüfung
 - keine Verantwortung und Bounces
- nach Weiterleitung schon verloren

ilpostino.jpberlin.de



pD9E2FC4C.dip.t-dialin.net



Bounce
an falsche
Absenderadresse



MX für uplug.de:
mail.variomedia.de



Listenserver:
mail.asta.uni-potsdam.de

REJECT

Maßnahmen

simple Checks, keine False Positives

- HELO/EHLO
 - *entweder*: full-qualified domain name
 - *oder*: adress literal [123.45.67.89]
 - *nicht* localhost oder mein eigener Hostname
- Sender- & Empfängeradressen
 - full-qualified domain name
 - MX-Eintrag vorhanden
 - MX-Eintrag mit öffentlicher IP
(kein 127.0.0.1, kein RFC1918-Netz)
 - gültiger lokaler Empfänger (!)
 - → Mailausgang nur nach Authentifizierung

weitere Maßnahmen

meist DNS-basiert, False Positives möglich

- Blacklists (RBLs und RHSBLs)
- HELO mit DNS-Eintrag
- Client mit DNS-Eintrag (forward *und* reverse)
- rfc-ignorant.org

Und sonst noch...

- Greylisting
- für Postfix: policyd-weight
- für Server: lokaler dnscache

CRM114

- Filtersprache zur Text-Klassifizierung
- verschiedene Klassifizierungsalgorithmen
- wichtigste Anwendung: Spamerkennung mit `mailreaver.crm`
- sehr gute Erkennungsraten (99,9%)



Installation in Kurzform

Kommandos:

```
mkdir ~/.crm114
cp mailfilter.cf rewrites.mfp *.crm ~/.crm114
cd ~/.crm114
cssutil -b -r spam.css
cssutil -b -r nonspam.css
touch priolist.mfp
$EDITOR mailfilter.cf
$EDITOR rewrites.mfp
```

Konfiguration in mailfilter.cf. Darin z. B.:

```
:add_headers: /yes/
:text_cache: /reaver_cache/
:spam_flag_subject_string: //
:accepted_mail_exit_code: /0/
```

Spamassasin-Plugin

- Problem: Programmaufruf & Pipe
gut für procmail, aber schlecht für Mailserver mit Amavis
- ⇒ Plugin geschrieben
- Unterstützt einige SA-Features wie
 - dynamischer Score
 - Training per SA

offene Probleme

- beste SA-Score-Berechnung gesucht
- für jede Mail wird eigener Prozess gestartet
(nicht zu ändern ohne daemonized CRM114)
- Patch nötig: CRM114-Header in Amavisd

neuer alter Spam-Trend: PDFs

- Versand aus Botnetzen.
⇒ Ein Restriktiver Mailserver lässt fast keine rein.
- Clamav-Signaturen von SaneSecurity
- SA-Plugins:
 - FuzzyOCR-Erweiterung von Christian Holler (Bild-Export mit pdftops & pstopnm, dann OCR)
 - PDFText von James MacLean (Text extrahieren mit pdftotext, pdfinfo, pdfimage & gocr)
 - PDFInfo von Dallas Engelken (eigene Parsing-Funktion prüft Checksummen)

⇒ weiter geht's mit XLS- und ZIP-Dateien...

Links

- Postfix Anti-UCE Cheat Sheet
- CRM114 - the Controllable Regex Mutilator
- SpamAssassin CustomPlugins