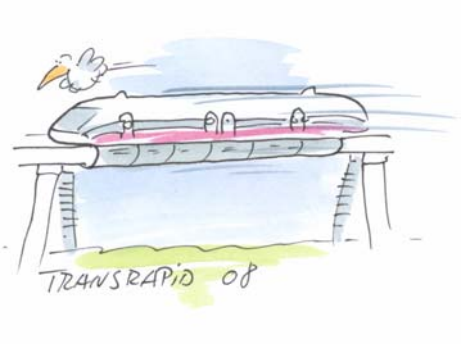


2B01 Spamabwehr am Mailrelayer mit Postfix unter Linux

Ansgar Schlüter, IABG mbH Aussenstelle Lathen

DECUS IT-Symposium, Düsseldorf/Neus 6. April 2005

Parlez vous SMTP ?

```
<< 220 mail.mustermann.de ESMTP
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<chef@domain.de>
<< 250 Ok
>> RCPT TO:<user@mustermann.de>
<< 250 Ok
>> DATA
<< 354 End data with <CR><LF>.<CR><LF>
>> To:chef@mustermann.de
>> Subject:Hallo
>>
>> Tach auch
>> .
<< 250 Ok
>> QUIT
<< 221 Bye
```

Grundprinzip Spamabwehr

- Spamabwehr so früh wie möglich durchführen, um Resourcen zu sparen
- Keine automatische Löschung von E-Mails (!)
- REJECTS (Annahmeverweigerung) nur während des SMTP-Dialogs
- Weiterführende Prüfungen nach dem SMTP-Dialog werden nur im Header gekennzeichnet und die E-Mail dem Empfänger zugestellt

IABG

Beispiel Spammailheader

```
Return-Path: <aaqpsp@adelphia.net>
Received: from mr.mustermann.de (mr.mustermann.de [192.168.10.1])
    by mailhost.mustermann.de (Postfix) with ESMTP id 3A72090602E5
    for <user@mailhost.mustermann.de>; Sun, 27 Jun 2004 05:26:29 +0200 (CEST)
Received: by mr.mustermann.de (Postfix, from userid 1001)
    id 0B58840506DC; Sun, 27 Jun 2004 05:26:27 +0200 (CEST)
Received: from zdfjw.adelphia.net (unknown [67.119.9.22])
    by mr.mustermann.de (Postfix) with SMTP id 174A44016EAB
    for <user@mustermann.de>; Sun, 27 Jun 2004 05:26:04 +0200 (CEST)
Message-ID: <GMJGICEWSFFXIDZRGGFFBVE@charter.com>
From: "Kristopher Terry" <aaqpsp@adelphia.net>
To: user@mustermann.de
Subject: Soma (And 300 Other Drugs) shipped overnight shafer
Date: Sun, 27 Jun 2004 06:16:57 +0200
X-Mailer: charm conant
junction-subtlety: delightful soldier trombone
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on mr.mustermann.de
X-Spam-Level: *
X-Spam-Status: No, hits=1.5 required=5.0 tests=BIZ_TLD,HTML_70_80,
    HTML_MESSAGE,MIME_QP_LONG_LINE autolearn=no version=2.63
X-Sanitizer: Mustermann mail filter
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="MIMEStream=_0+148945_1957804559857_85650093849"
X-Virus-Scanned: by AMaViS-perl11-milter (http://amavis.org/)
```

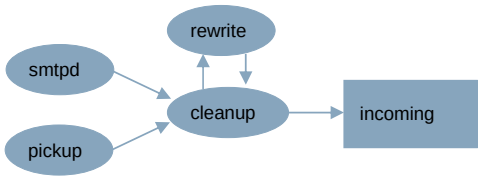

IABG

MTA postfix

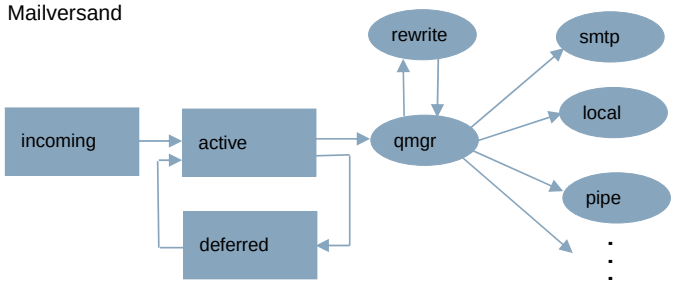
- Entwickelt als sendmail-Ersatz von Wietse Venema
- Modulares Konzept
- Einfach konfigurierbar durch lesbare ASCII-Dateien
  - master.cf für die Prozesskonfiguration
  - main.cf für die Verhaltenskonfiguration
- Security als Entwicklungsprinzip
- chroot-fähig

Modularer Aufbau von Postfix

Mailempfang



Mailversand



Prüfungen (restriction)

- Die IP-Nummer (smtpd_client_restriction)
- HELO-Prüfung (smtpd_helo restriction)
- MAIL FROM: -Prüfung (smtpd_sender_restriction)
- RCPT TO:-Prüfung (smtpd_recipient_restriction)
- Inhaltsprüfung der Mail (header-, body- bzw. mime_checks)
- Nutzung von Tabellen

z.B. /etc/postfix/sender_access

```
# Mails von dieser Adresse immer erlauben
postmaster@myfriend.de          OK
# Bekannter Spammer wird geblockt
@spam.cn                        REJECT
```

- Defaultmäßig führt Postfix alle Prüfungen erst nach dem RCPT TO: durch. Erst jetzt liegen alle wichtigen Informationen vor.

IABG

smtpd_client_restriction

- reject_unknown_client
  REJECT, wenn für den Client im DNS kein PTR, also kein Name zur IP-Nummer gesetzt ist.

- check_client_access typ:mapname
  Tabelle mit direktem REJECT oder OK
  z.B. /etc/postfix/client_access

```
# Mails von befreundeter Domain immer herein lassen
mail.myfriend.de                OK
# Blocken eines bekannten Spamserver
111.222.111.222                 REJECT
```

```
<< 220 mustermann.de
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<...>
<< 250 Ok
>> RCPT TO:<...>
<< 250 Ok
```


IABG

smtpd_helo_restriction

- reject_unknown_hostname
  blockt die Mail, wenn für den HELO-Hostnamen im DNS kein A- bzw. MX-Record existiert.
- reject_non_fqdn_hostname
  blockt die Mail, wenn der HELO-Hostname kein *Fully Qualified Domain Name* ist.
- reject_invalid_hostname
  blockt die Mail, wenn der HELO-Hostname in einer ungültigen Syntax angegeben wird (Sonderzeichen, etc.)
- check_helo_access typ:mapname
  z.B. /etc/postfix/helo_access
  # blocken von HELOs mit unserem Domainnamen
  mustermann.de 550 You are not in mustermann.de
  111.222.0.1 550 You are not in mustermann.de

<< 220 mustermann.de
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<...>
<< 250 Ok
>> RCPT TO:<...>
<< 250 Ok

IABG

smtpd_sender_restriction

- reject_unknown_sender_domain
  blockt die Mail, wenn für den Senderadresse im DNS kein A- bzw. MX-Record existiert
- reject_non_fqdn_sender
  blockt die Mail, wenn die Senderadresse kein *Fully Qualified Domain Name* ist.
- reject_unverified_sender
  blockt die Mail, wenn eine Probemail mit der Senderadresse bounced oder nicht erreichbar ist.
- check_sender_access typ:mapname
  z.B. /etc/postfix/sender_access
  # Mails von dieser Adresse immer erlauben
  postmaster@myfriend.de OK
  # Bekannter Spammer wird geblockt
  @spam.cn REJECT

<< 220 mustermann.de
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<...>
<< 250 Ok
>> RCPT TO:<...>
<< 250 Ok

IABG

smtpd_recipient_restriction (1/2)

- reject_unauth_destination
  blockt die Mail, wenn Postfix nicht für diese Empfangsdomäne zuständig ist.
- reject_unknown_recipient_domain
  blockt die Mail, wenn für den Empfängeradresse im DNS kein A- bzw. MX-Record existiert
- reject_non_fqdn_recipient
  blockt die Mail, wenn die Senderadresse kein *Fully Qualified Domain Name* ist.

<< 220 mustermann.de
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<...>
<< 250 Ok
>> RCPT TO:<...>
<< 250 Ok

IABG

smtpd_recipient_restriction (2/2)

- reject_unverified_recipient
  blockt die Mail, wenn eine Probemail mit der Senderadresse bounced oder nicht erreichbar ist.

<< 220 mustermann.de
>> HELO host.domain.de
<< 250-mail.domain.de
>> MAIL FROM:<...>
<< 250 Ok
>> RCPT TO:<...>
<< 250 Ok

- check_recipient_access typ:mapname
  z.B. /etc/postfix/recipient_access
  # Mails fuer diese Adresse immer erlauben
  postmaster@mustermann.de OK
  abuse@mustermann.de OK
  # ex-Mitarbeiter
  user1@mustermann.de REJECT

IABG

Header-, Body- und Mimeprüfungen

- Ausführung erfolgt nach dem Empfang der Daten
- header_checks = pcre:/etc/postfix/maps/header_check.pcre

/^Subject:.*100\% Free/	REJECT Woah! Free?
/^From:.*spammer@domain\.de/	REJECT Geh weg, Spammer.
/^X-Mailer:.*Microsoft/	REJECT Get a _real_ MUA.

- body_checks = pcre:/etc/postfix/maps/body_check.pcre

/See the attached file for details/	REJECT Sobig Virus gefunden.
/Get your free/	REJECT Free? No, thanks.

- mime_header_checks pcre:/etc/postfix/mime_header_check.pcre

/name=[^>]*\.exe/	REJECT Keine .exe Files bitte.
/name=[^>]*\.bat/	REJECT Keine .bat Files bitte.
/name=[^>](screensaver|movie)\.zip/	REJECT Sobig Virus gefunden.

IABG

Realtime Blacklist (RBL)

- **reject_rbl_client domain.tld**
  Block die Mail, wenn der SMTP Client einen DNS Rekord vom Typ A unter domain.tld hat. Ein RBL ist eine Real-time Blacklist (IP basiert).
- **reject_rhsbl_client domain.tld**
  Block die Mail, wenn der SMTP Client einen DNS Rekord vom Typ A unter domain.tld hat. Ein RHSBL ist eine Real-time Blacklist (Domain basiert).
- **reject_rhsbl_sender domain.tld**
  Block die Mail, wenn der Sender einen DNS Rekord vom Typ A unter domain.tld hat.

IABG

Beispielkonfiguration Ausschnitt aus main.cf

```
smtpd_helo_required = yes
strict_rfc821_envelopes = yes
disable_vrfy_command = yes

smtpd_recipient_restrictions =
      permit_mynetworks,
      reject_unauth_destination,
      reject_unknown_client,
      reject_invalid_hostname,
      reject_non_fqdn_hostname,
      reject_unknown_hostname,
      reject_unknown_sender_domain,
      reject_non_fqdn_sender,
      reject_unverified_sender,
      reject_non_fqdn_recipient,
      reject_unknown_recipient_domain,
      reject_unverified_recipient,
      check_client_access          hash:/etc/postfix/client_access,
      check_helo_access            hash:/etc/postfix/helo_checks,
      check_sender_access          hash:/etc/postfix/sender_access,
      check_recipient_access       hash:/etc/postfix/recipient_access,
      reject_rbl_client            sbl-xbl.spamhaus.org,
      permit

header_checks = pcre:/etc/postfix/header_checks.pcre
body_checks = pcre:/etc/postfix/body_checks.pcre
mime_header_checks pcre:/etc/postfix/maps/mime_header_check.pcre
```


IABG

Reelle Konfiguration (Ausschnitt aus main.cf)

```
smtpd_helo_required = yes
strict_rfc821_envelopes = yes
disable_vrfy_command = yes

smtpd_recipient_restrictions =
      permit_mynetworks,
      reject_unauth_destination,
      reject_unknown_sender_domain,
      reject_non_fqdn_sender,
      reject_non_fqdn_recipient,
      reject_unknown_recipient_domain,
      check_client_access          hash:/etc/postfix/client_access,
      check_helo_access            hash:/etc/postfix/helo_checks,
      check_sender_access          hash:/etc/postfix/sender_access,
      check_recipient_access       hash:/etc/postfix/recipient_access,
      reject_rbl_client            sbl-xbl.spamhaus.org,
      permit

header_checks = pcre:/etc/postfix/header_checks.pcre
body_checks = pcre:/etc/postfix/body_checks.pcre
mime_header_checks pcre:/etc/postfix/mime_header_check.pcre
```

Resultat: Mit dieser Konfiguration läßt sich ca. 5 - 10% der Spam abwehren

IABG

Definition eigener Restriktionen

- Mit den eingebauten Restriktionen kann nur die jeweilige Phase des SMTP-Dialoges geprüft werden.
- Mit der Definition eigener Restriktionen können Verknüpfung über die Phasen des SMTP-Dialoges hergestellt werden

smtpd_restriction_classes = myrestriction, …

myrestriction =
    check_sender_access typ:mapname

In einer Tabelle Verweis auf eigene Restriktion
    …
    domain.tld   myrestriction
    …

IABG

smtpd_restriction_classes (Beispiel freemail)

- Quercheck zwischen Senderadresse und Clientadresse

smtpd_restriction_classes = freemail_hotmail

freemail_hotmail =
check_client_access   pcre:/etc/postfix/freemail_hotmail

- :/etc/postfix/freemail_hotmail
  /(^|\.)hotmail\.com$/ DUNNO
  /./ REJECT You are not from Hotmail

- /etc/postfix/freemail_check
  # Check hotmail
  hotmail.com freemail_hotmail
  […]

smtpd_recipient_restrictions =
    [..]
    check_sender_access hash:/etc/postfix/freemail_check,
    [..]

IABG

smtpd_restriction_classes (Beispiel User)

- Erweiterte Restriktionen nur für genannte Empfänger

```
smtpd_restriction_classes = freemail_hotmail, user_uce_check

user_uce_check =
    […]
    reject_unknown_client,
    reject_invalid_hostname,
    check_sender_access          hash:/etc/postfix/freemail_check,
    […]
```

- /etc/postfix/uce_check
  ```
  # Check hotmail
  userA@mustermann.de        user_uce_check
  […]
  ```

```
smtpd_recipient_restrictions =
    [..]
    check_recipient_access hash:/etc/postfix/uce_check,
    [..]
```

- **Resultat der eigenen Restriktion: weitere 10-50 % Spam ausfiltern**

IABG

Policyserver

- Mit Postfix Version 2.1 ist die *SMTP access policy delegation* eingeführt.
- Externer Prozess entscheidet über REJECT,OK, etc.
- Postfix übermittelt dazu alle bis zum RCPT TO: verfügbaren Informationen.
  z.B: helo_name=some.domain.tld
  queue_id=8045F2AB23
  sender=foo@bar.tld
  recipient=bar@foo.tld
  client_address=1.2.3.4
  client_name=another.domain.tld
  size=12345
- Eröffnet flexible Kontrollmöglichkeiten
- Etliche Policyserver verfügbar (z.B. Greylisting, SPF, etc)

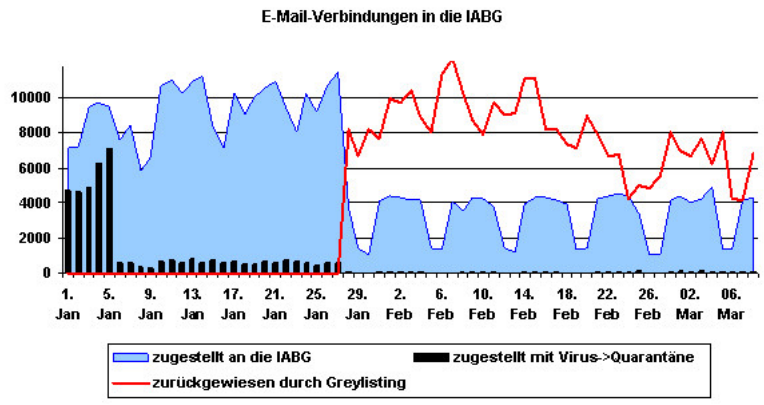
```
smtpd_recipient_restrictions =
    [..]
    check_policy_service       unix:private/policy ,
    [..]
```


IABG

Greylisting

- Momentan sehr wirkungsvolle Methode zur Abwehr von Spam (> 90 %)
- Nutzt die Tatsache aus, dass SMTP beim Transport nicht verlässlich ist.
- Auswertung des Triplets
  - Client IP-Adresse
  - Envelop Senderadresse
  - Envelop Empfängeradresse
- Auswertemethode: (Auszug aus dem Whitepaper zu Greylisting)
  - „If we have never seen this triplet before,
  - then refuse this delivery and any others
  - that may come within a certain period of time
  - with a temporary failure.“

Auswirkung Greylisting



Weiterleitung zu externen Prüfprogrammen (content_filter)

- Nutzung des Content-Filter zur Prüfungen auf Spam oder auch auf Viren
- Mail ist jetzt komplett angenommen worden
- Keine REJECTs, nur noch Kennzeichnung der Mail als spamverdächtig
- Populärer Content-Filter ist amavisd-new, eine Kombination aus Virenscanner und Spamassassin
- Spamassassin nutzt Bayesfilter und ist lernfähig,

```
#
#==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
#==========================================================================
smtp                inet  n  -  n  -  2       smtpd -o content_filter=smtp:[localhost]:10024
# Instanz zum Empfang der Mails vom content_filter
localhost:10025 inet  n  -  n  -  -       smtpd -o content_filter=
```


IABG

Hardware und Software

- 1HE Server mit Pentium III 933 MHz und 384 MB RAM
- SuSE Linux 9.2 Professional
- Minimalinstallation
- Nicht benötigte Dienste deaktivieren bzw. deinstallieren
- Für Greylisting (postgrey) muss ein zusätzliches Paket von CPAN installiert werden
- Firewall lässt nur Port 25 vom Internet durch
- Sicherung des Rechners mit tripwire
- Postfix smtpd läuft in einer chroot-Umgebung

IABG

Q & A

Vielen Dank für Ihre Aufmerksamkeit!

Fragen

&

Antworten

IABG