Postfix: Postfix: Greylisting mit Postgrey (SuSE 9.x)

Danke

an Michael als Testperson!

Seine unten genannten Verbesserungen sind integriert.

Problem:

Der alltägliche Spam nimmt überhand. Spamfilter wie SpamAssassin können gar nicht mehr die Regeln so schnell nachladen oder Spams lernen um wirklich effektiv zu arbeiten. SPF ist zwar auch eine Möglichkeit, könnte aber erwünschte Emails aussperren.

Eine effektive Lösung bittet dazu Greylisting.

Funktion von Greylisting:

Es block jede Email beim ersten Versuch ab. Erst wenn diese Email ein zweites Mal eingeliefert wird, wird sie auch angenommen. Das funktioniert, weil jeder echte Email-Server mehrmals versucht seine Emails bei dem Empfänger abzuliefern. Schließlich könnte ja mal ein Server ausgefallen oder überlastet sein. Spam-Versender-Programme hingegen liefern einfach nur Daten ein, ohne die Antwort zu registrieren. Es versucht also abgelehnte Emails i.d.R. kein zweites Mal einzuliefern. Und deshalb ist Greylist so effektiv.

Installation:

Für Postgrey unter SuSE gibt es bisher kein fertiges RPM-Paket. Und selbst, wenn es mal eins geben wird, so wird es wohl eher für openSUSE 10 oder höher sein. Daher bringe ich hier eine Anleitung inkl. start-Script *für SuSE 9.x* und alle anderen Versionen die noch ohne Postgrey-Paket daher kommen.

Postgrey nutzt eine Berkeley-DB zum Speichern seiner Daten und verwaltet sie vollkommen autonom. Die passenden Libraries und Perl-Module sind meistens schon installiert. Sollten später beim Start von postgrey Fehler mit dbm-Zugriffen auftauchen, schaut erstmal im yast nach, ob alle nötigen Pakete vorhanden sind.

Download & Installation

Erstmal überprüfen wir die neueste Version von Postgrey und setzten ggf. den aktuellen Download-Pfad hier ein:

```
#Download
cd /usr/local/src
wget http://postgrey.schweikert.ch/pub/postgrey-1.31.tar.gz
tar xzf postgrey-1.31.tar.gz
cd postgrey-1.31

#Installation
cp postgrey /usr/local/sbin/.
cp postgrey_whitelist_clients /etc/postfix/.
cp postgrey_whitelist_recipients /etc/postfix/.
#wer einen Report lesen will
cp contrib/postgreyreport /usr/local/bin/.
#nötiges Verzeichnis anlegen
mkdir /var/spool/postfix/postgrey
chown postfix /var/spool/postfix/postgrey
chmod 700 /var/spool/postfix/postgrey
```

Theoretisch steht einem direkten Aufruf nichts im Wege. Aber da Postgrey als Daemon läuft, sollte es auch ein passendes Startscript erhalten:

```
#Startscript
cd /usr/local/src
wget http://www.huschi.net/download/rcpostgrey.tgz
tar xzf rcpostgrey.tgz
mv rcpostgrey /usr/local/sbin/.
#verlinken und automatischen Start setzen
ln -s /usr/local/sbin/rcpostgrey /etc/init.d/postgrey
insserv postgrey

#testen
/etc/init.d/postgrey
#Auftretende Fehler sofort untersuchen!
#ggf. CPAN-Module nachinstallieren:
cpan -i Net::Server
cpan -i IO::Multiplex
cpan -i BerkeleyDB
```

Nun sollte Postgrey als Server-Prozess laufen und an Port 60000 lauschen. Wir überprüfen es mit folgenden 2 Befehlen:

```
#Software
ps aux|grep postgrey
#Netzwerk
netstat -lpn | grep 60000
```

Integration in Postfix

Um Postgrey in den MTA von Postfix zu integrieren benötigt es lediglich eine kleine Änderung in der `/etc/postfix/main.cf`. Die Direktive `smtpd_recipient_restrictions` muß wie folgt *ergänzt* werden:

```
# check_policy_service inet:127.0.0.1:60000
```

Danach muß Postfix seine Konfiguration neu einlesen (`/etc/init.d/postfix reload`) und schon ist Postgrey aktiviert.

Die ersten Ergebnisse kann man recht schnell im Maillog vorfinden.

Wie oben schon angedeutet, kann man mit `postgreyreport` oder auch mit anderen Tools kleine Statistiken ausgeben lassen.

Eindeutige ID: #1232
huschi
2010-05-27 07:44