

Postfix: Postfix: Greylisting mit Postgrey (Debian)

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 Postfix unter Debian gibt es mit dem Paket Postgrey eine einfache und effektive Lösung. Postgrey nutzt eine [Berkeley-DB](#) zum Speichern seiner Daten und verwaltet sie vollkommen autonom.

```
#Installation (Abhängigkeiten mit installieren!)
```

```
apt-get install postgrey
```

```
#Postgrey wird i.d.R. direkt gestartet.
```

```
#Testen ob er wirklich da ist:
```

```
netstat -lpn | grep 60000
```

```
#Einbinden in Postfix:
```

```
edit /etc/postfix/main.cf
```

```
# smtpd_recipient_restrictions ergänzen um folgenden Eintrag:
```

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

```
#Postfix neu laden:
```

```
/etc/init.d/postfix reload
```

Die ersten Ergebnisse kann man direkt im [Maillog](#) beobachten.

Zum Testen am besten eine Email von GMX/Web.de/Yahoo/etc. an den Server schicken und im Logfile beobachten.

Eindeutige ID: #1213

huschi

2007-02-22 10:55