

Spam, Viren und viele sonstige Mails verstopfen unsere Mail Postfächer. Eine interessante Methode bietet hier Greylisting.

### Definition Greylisting

Auszug aus dem deutschen Wikipedia Artikel:

Der Begriff **Graue Liste** bzw. **Greylisting** (brit.)/**Graylisting** (USA) bezeichnet eine Form der Spam-Bekämpfung bei E-Mails, bei dem E-Mail von unbekanntem Absendern temporär abgewiesen und erst nach einem zweiten Zustellversuch angenommen wird.

### Funktionsweise

Das Prinzip ist so einfach und doch so wirkungsvoll. Spam Versender haben nicht die Zeit zu überprüfen, ob eine Mail auch wirklich ankommt. Es zählt einzig und alleine die Menge der Mails, die versendet wird. Dabei bleibt keine Zeit zum überprüfen, ob die Mail auch wirklich ankommt. Auch viele Mail-Viren überprüfen nicht, ob eine Mail auch wirklich ankommt.

Gerade diesen Punkt kann man mit Greylisting zunutze machen. Beim Erstkontakt merkt sich der SMTP Server ein sogenanntes Triplet (drei Parameter) bestehend aus Absenderadresse, Zieladresse und Absender-IP-Adresse. Der erste Zustellversuch wird aber gleich abgeblockt, bzw. die Mail wird nicht angenommen.

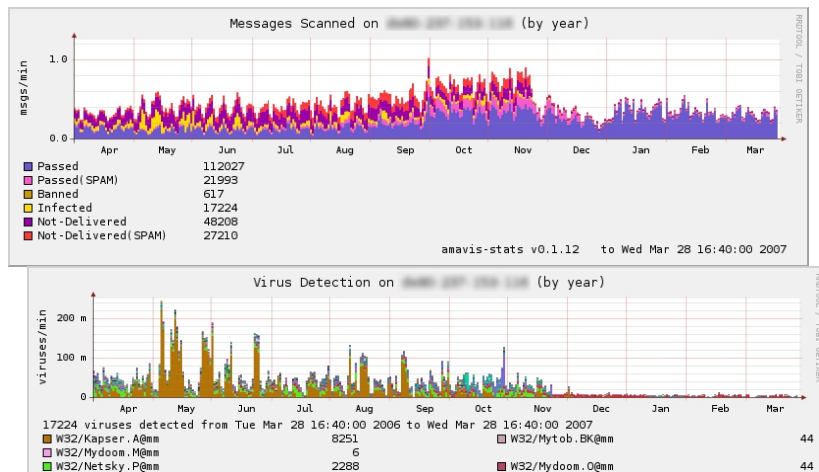
Kommt das gleiche Triplet nach einer eingestellten Wartezeit wieder vor, wird die Mail angenommen und entsprechend zugestellt.

Das Triplet, das gerade durch seinen zweiten Zustellversuch bewiesen hat, dass es ordentlich arbeitet, wird in einer Datenbank abgelegt. Dadurch werden weitere Mails ohne Verzögerung gleich zugestellt.

## Vorteile

Der gravierende Vorteil dieser Methode liegt klar auf der Hand. Massenemails kommen nicht mehr durch und viele Mail-Viren kommen auch nicht durch. Aktuelle Zahlen sprechen von einer Reduzierung von Spam Mails auf ein Zehntel.

Zur Belegung dieser Zahlen hier zwei Grafiken, die verdeutlichen, wie wirksam der Schutz funktioniert (und raten sie mal, wann Greylisting aktiviert wurde).



## Wie implementiert man Greylisting in Postfix?

Persönlich favorisiere ich MySQL als Datenbank im Hintergrund. Viele Applikationen brauchen eine Datenbank und warum sollte man die vorhandene nicht auch dafür benützen.

### Installation unter Gentoo

Unter Gentoo gibt es einen entsprechenden Ebuild. Mittels folgendem Kommando kann man überprüfen, ob auch alles passend eingestellt ist:

```
# emerge -pv sqlgrey
```

These are the packages that would be merged, in order:

Calculating dependencies... done!

```
[ebuild N ] dev-perl/IO-Multiplex-1.08 14 kB
[ebuild N ] dev-perl/net-server-0.94 81 kB
[ebuild N ] dev-perl/Carp-Clan-5.3 16 kB
[ebuild N ] dev-perl/Bit-Vector-6.4 128 kB
[ebuild N ] dev-perl/Date-Calc-5.4 201 kB
[ebuild N ] mail-client/mailx-support-20030215 8 kB
[ebuild U ] sys-devel/automake-wrapper-3-r1 [1-r1] 0 kB
[ebuild U ] sys-devel/autoconf-wrapper-4-r3 [3.2] 0 kB
[ebuild U ] sys-devel/m4-1.4.7 [1.4.4] USE="nls" 499 kB
[ebuild U ] sys-devel/autoconf-2.61 [2.59-r7] USE="-emacs" 1,364 kB
[ebuild N ] dev-perl/Locale-gettext-1.05 7 kB
[ebuild N ] sys-apps/help2man-1.36.4 USE="nls" 83 kB
[ebuild NS ] sys-devel/automake-1.10 872 kB
[ebuild N ] net-libs/liblockfile-1.06-r2 31 kB
[ebuild N ] mail-client/mailx-8.1.2.20040524-r1 126 kB
[ebuild N ] mail-filter/sqlgrey-1.7.4 USE="mysql -postgres -sqlite" 55 kB
```

Total size of downloads: 3,492 kB

Wichtig ist hierbei, dass bei sqlgrey in der letzten Zeile auch MySQL aktiviert ist, d.h. ohne Minus Zeichen davor. Die Pakete davor sind Abhängigkeiten, die bei Ihnen anders aussehen kann. Die abhängigen Pakete sind für die Funktion des Paketes notwendig.

Steht in Ihrem Fall mysql nicht mit in der sqlgrey Zeile, gibt es 3 Möglichkeiten. Die einfachste Möglichkeit besteht im Ändern der USE Zeile in der Datei /etc/make.conf. Hier einfach mysql hinzufügen. Die zweite Möglichkeit ist das Ändern oder erstellen der Datei /etc/portage/package.use mit folgendem Inhalt:

```
mail-filter/sqlgrey mysql
```

Oder man führt folgendes aus:

```
USE="mysql" emerge -pv sqlgrey
```

Um nun das Paket zu installieren, entfernt man einfach von obigem Aufruf die Parameter "-pv" und schon legt das System los.

### Die Schnelle Installation

Nach der Installation muss die Datenbank eingerichtet werden.

```
emerge --config sqlgrey
```

Configuring pkg...

- \* SQLgrey database backend configuration
- \* Please select where SQLgrey database will run:
  - \* [l] Database backend runs on localhost
  - \* [r] Database backend runs on remote host
  - \* [x] Exit
- \* Press one of the keys [l,r,x]:
- \* local setup
- \* Generating random database user password...
- \* Creating SQLgrey database backend data and configuration
- \* Please select what kind of database you like to use:
  - \* [m] MySQL
  - \* [x] Exit
- \* Press one of the keys [m,x]:
- Enter password: \* MySQL database backend
- \* If prompted for a password, please enter your MySQL root password
- \* Creating SQLgrey MySQL database "sqlgrey" and user "sqlgrey"
- \* Changing SQLgrey configuration in sqlgrey.conf
- \* Note: the database password is stored in /etc/sqlgrey/sqlgrey.conf

Die Fragen bei der Konfiguration sind mit l (localhost) und m (MySQL) zu beantworten. Danach

## Greylisting in Postfix mit MySQL - baecker.com

Geschrieben von: Michael Bäcker

Freitag, den 08. Januar 2010 um 13:20 Uhr - Aktualisiert Freitag, den 08. Januar 2010 um 13:49 Uhr

---

gibt man noch sein root Passwort der MySQL Datenbank an.

Die Konfigurationsdatei wird automatisch mit den richtigen Werten befüllt. Danach muss Postfix noch angepasst werden, dass das Greylisting auch verwendet wird. In der Datei `/etc/postfix/main.cf` muss folgendes an passender Stelle eingefügt werden:

```
smtpd_recipient_restrictions =  
...  
check_policy_service inet:127.0.0.1:2501
```

Soweit so gut. Jetzt muss noch alles aktiviert werden oder auch neu gestartet werden:

```
/etc/init.d/sqlgrey start  
rc-update add sqlgrey default  
/etc/init.d/postfix restart
```

Ab hier sollte man sich folgendes Logfile genauer ansehen ob alles geklappt hat:

```
/var/log/mail.info oder /var/log/mail.log
```

Hier sollten nun nach und nach die Meldungen kommen, dass der Sender erst mal abgewiesen wurde. Nach weiteren Minuten, wenn der selbe Sender nochmals sendet, sollte er durchgelassen werden.

Weitere Beobachtungsmöglichkeiten befinden sich in der Datenbank.

Die Tabelle `connect` enthält alle Verbindungsversuche, die Tabelle `from_awl` die erfolgreichen Verbindungen (2x Connect und Zustellung der Mail).

## Greylisting in Postfix mit MySQL - baecker.com

Geschrieben von: Michael Bäcker

Freitag, den 08. Januar 2010 um 13:20 Uhr - Aktualisiert Freitag, den 08. Januar 2010 um 13:49 Uhr

---

Als weitere Lektüre sind die README Dateien zu empfehlen, die Tips & Tricks für das Feintuning mittels der weiteren Tabellen beinhalten.

Viel Spass beim Konfigurieren und dem zukünftig Spamärmeren Postfach.

[Joomla SEF URLs by Artio](#)