

Spamdyke als Anti-Spam-Lösung in eine Plesk-Installation mit Qmail integrieren

cplinux // 27.10.2009 16:22

Kategorie: **Plesk**

Im Folgenden werde ich zeigen, wie man die Anti-Spam-Lösung **spamdyke** in eine bestehende Plesk-Installation integriert. Standardmäßig verwendet Plesk den Maildienst Qmail.

Zuerst einmal stellt man sicher, dass alle benötigten Pakete auf dem System installiert sind. Auf einem Debian-System erledigt man das mit:

```
apt-get install gcc make libc-dev
```

Jetzt lädt man sich die neueste Version von Spamdyke herunter:

<http://www.spamdyke.org/download.html>

Aktuell ist 4.0.10 die neueste Version. Man kann die Datei auch direkt auf dem Server herunterladen und entpacken:

```
wget http://www.spamdyke.org/releases/spamdyke-4.0.10.tgz
tar -xvzf spamdyke-4.0.10.tgz
cd spamdyke-4.0.10/spamdyke
```

Jetzt muß man das Paket kompilieren:

```
./configure
make
```

Nach den beiden Befehlen sollte sich jetzt die ausführbare Datei spamdyke in dem Verzeichnis befinden. Diese kopiert man jetzt z.B. in /usr/local/bin für die spätere Verwendung:

```
cp spamdyke /usr/local/bin/
```

Soweit so gut, Spamdyke ist installiert! Jetzt muß es noch in die Plesk-Konfiguration eingebunden werden.

Normalerweise sollte das System xinetd verwenden. Zuerst sichert man die Original-Dateien:

```
cp /etc/xinetd.d/smtp_psa /etc/xinetd.d/smtp_psa.orig
cp /etc/xinetd.d/smtps_psa /etc/xinetd.d/smtps_psa.orig
```

Jetzt editiert man die beiden Dateien **smtp_psa** und **smtps_psa**, z.B. mit nano, vim, etc.

Nun fügt man den folgenden Befehl ein und zwar direkt vor var/qmail/bin/qmail-smtpd.

Bitte dabei darauf achten, dass der Befehl nicht in eine neue Zeile umbricht.

```
/usr/local/bin/spamdyke -f /etc/spamdyke.conf
```

Danach sollte man xinetd neu starten:

```
/etc/init.d/xinetd restart
```

ACHTUNG!

Je nach Plesk-Version kann es sein, dass das System **inetd** statt **xinetd** verwendet.

Dann gilt es den Befehl

```
/usr/local/bin/spamdyke -f /etc/spamdyke.conf
```

in der Datei **/etc/inetd.conf** einzutragen, **direkt vor /var/qmail/bin/qmail-smtpd.**

Den Neustart erledigt man mit:

```
/etc/init.d/inetd restart
```

Die **Konfigurationsdatei für Spamdyke** fehlt natürlich noch. Dazu legen wir die Datei **/etc/spamdyke.conf** an, mit folgendem Inhalt:

```
log-level=2
local-domains-file=/var/qmail/control/rcpthosts
max-recipients=20
idle-timeout-secs=60
graylist-dir=/var/qmail/spamdyke/graylist
graylist-min-secs=300
graylist-max-secs=1814400
sender-blacklist-file=/var/qmail/spamdyke/blacklist_senders
sender-whitelist-file=/var/qmail/spamdyke/whitelist_senders
recipient-blacklist-file=/var/qmail/spamdyke/blacklist_recipients
ip-in-rdns-keyword-file=/var/qmail/spamdyke/blacklist_keywords
ip-blacklist-file=/var/qmail/spamdyke/blacklist_ip
rdns-whitelist-file=/var/qmail/spamdyke/whitelist_rdns
ip-whitelist-file=/var/qmail/spamdyke/whitelist_ip
reject-empty-rdns
reject-unresolvable-rdns
greeting-delay-secs=5
check-dnsrbl=bl.spamcop.net
reject-missing-sender-mx
```

Die Konfiguration kann man natürlich noch etwas anpassen.

Die o.a. Konfiguration ist für den Anfang denke ich schon mal nicht schlecht. Eine vollständige Liste aller möglichen Optionen findet man hier:

<http://www.spamdyke.org/documentation/README.html>

Ok, jetzt gilt es, die fehlenden Verzeichnisse gemäß der Konfigurationsdatei anzulegen:

```
mkdir -p /var/qmail/spamdyke/graylist
touch /var/qmail/spamdyke/blacklist_ip
touch /var/qmail/spamdyke/blacklist_recipients
touch /var/qmail/spamdyke/whitelist_ip
touch /var/qmail/spamdyke/blacklist_keywords
touch /var/qmail/spamdyke/blacklist_senders
touch /var/qmail/spamdyke/whitelist_senders
touch /var/qmail/spamdyke/whitelist_rdns
```

Ich denke, die Namen der Dateien verdeutlichen selbst, wofür sie stehen. In die Datei "blacklist_ip" z.B. kann man z.B. zeilenweise die IP-Adressen eintragen, die man sofort blocken möchte.

Zu beachten ist, dass nach einer Änderung xinetd und qmail neu gestartet werden sollten, damit die Änderungen wirksam werden.

Die neu angelegten Dateien müssen nun noch die richtigen Berechtigungen bekommen:

```
chown -R qmail:nofiles /var/qmail/spamdyke
```

Für bereits existierende E-Mail-Konten müssen nun noch die entsprechenden Greylist-Ordner angelegt werden:

```
cd /var/qmail/spamdyke/graylist/
for i in `ls -l /var/qmail/mailnames`; do mkdir $i; done
chown -R qmail:nofiles /var/qmail/spamdyke
```

Damit das nicht für jede neu angelegte Domain wiederholt werden muß, erstellt man nun ein kleines Shell-Script, das danach im Plesk Event Manager eingetragen wird. Die Datei kann man z.B. in /usr/local/psa/bin anlegen: **/usr/local/psa/bin/create_greylist_folder.sh**

```
#!/bin/bash

# greylist folder
greylist_path="/var/qmail/spamdyke/greylist"

# add new folder
mkdir $greylist_path/$1

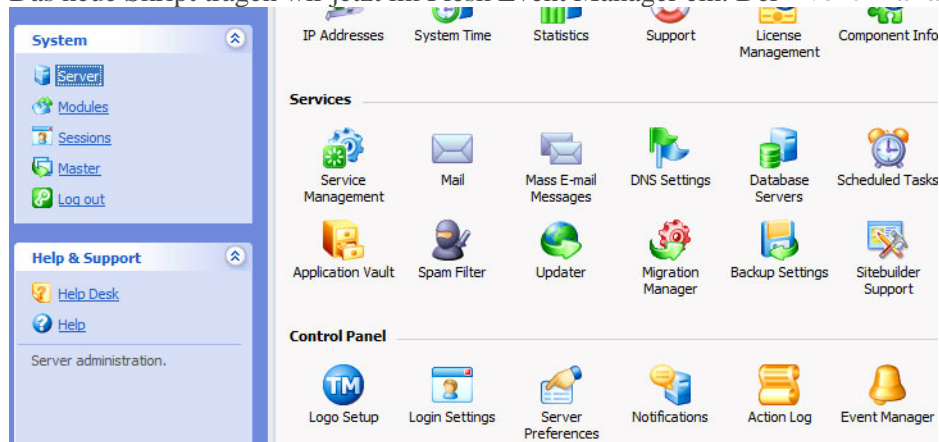
# create proper permissions
chown qmaild:nofiles $greylist_path/$1

exit
```

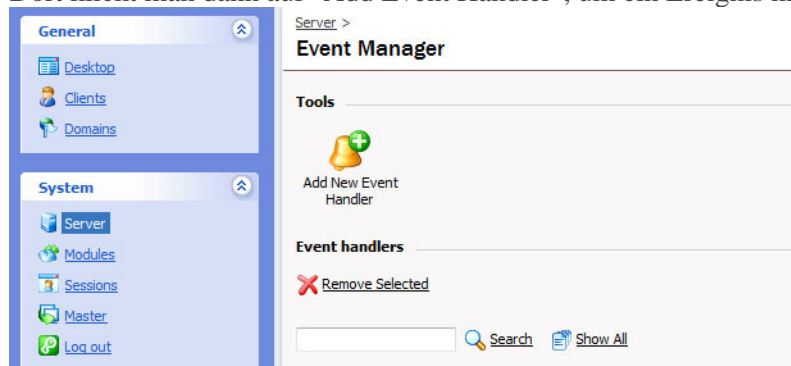
I.d.R. dürfte das Skript bereits root gehören. Es muß aber noch die entsprechenden Berechtigungen bekommen, damit es ausführbar ist:

```
chown root:root /usr/local/psa/bin/create_greylist_folder.sh
chmod 755 /usr/local/psa/bin/create_greylist_folder.sh
```

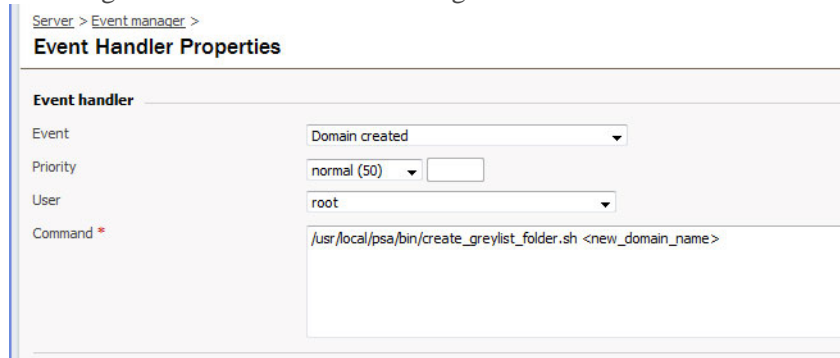
Das neue Skript tragen wir jetzt im Plesk Event Manager ein. Der **Event Manager** befindet sich im Bereich **Server**.



Dort klickt man dann auf "Add Event Handler", um ein Ereignis hinzuzufügen.



Jetzt trägt man das neue Event wie abgebildet ein:



Event	Domain created
Priorität	Normal

Benutzer	root
Befehl	/usr/local/psa/bin/create_greylist_folder.sh

Das war's! Jetzt sollte man sich die Logs ansehen! /var/log/mail.info bzw. /var/log/mail.log