Plesk

Spamdyke installieren auf Plesk 10/Debian 6.0 Server incl. Spamdyke Control Panel

http://www.spamdyke.org/

Installation:
Zuerst besorgen wir uns die gepatchte Spamdyke Version mit mysql Unterstützung von haggybear.de. Wer sich dort noch nicht registriert hat, der meldet sich dort zuerst an.

Nach der Registrierung laden wir uns das Spamdyke Control Panel 2.6 herunter.

```
cd /usr/local/src
```

```
wget http://www.haggybear.de/download/spamdyke-mysql.tgz
```

```
tar -xzf spamdyke-mysql.tgz
```

In den Faq finden wir den geänderten wrapper, den wir für Plesk 10 ebenfalls benötigen:

```
wget http://www.haggybear.de/download/wrapper/psa9/scp2.zip
```

Unter Debian 6.0 benötigen wir noch ein paar Libs und einen Compiler:

```
aptitude install gcc libssl-dev libmysqlclient-dev
```

Danach kann spamdyke kompiliert und nach /usr/local/bin installiert werden.

```
cd /usr/src/spamdyke-mysql/spamdyke
./configure
```

Diese beiden Ausgaben müssen unbedingt nach dem ./configure angezeigt werden:

```
checking for MySQL (for MySQL-Logging support)... yes
checking for MySQL includes (for MySQL-Logging support)...yes
```

```
make
make install
```

Jetzt werden wir noch einige Hilfsprogramme Compilieren. Diese Programme werden aber für das CP nicht benötigt.

```
cd /usr/src/spamdyke-mysql/utils
./configure && make
cp dnsa dnsany dnsany_libc dnsmx dnsns dnsptr dnssoa dnstxt domain2path domainsplit
/usr/local/bin
```

Konfiguration
Zunächst wird spamdyke nun mit einer sinnvollen Konfiguration versorgt.
Dazu wird eine Datei namens /etc/spamdyke.conf mit folgendem Inhalt angelegt:

```
touch /etc/spamdyke.conf
```

#für Spamdyke:
log-level=info

config-mysql-database=spamdyke
config-mysql-username=spamdyke
config-mysql-password=spamdyke

local-domains-file=/var/qmail/control/rcpthosts
tls-certificate-file=/var/qmail/control/servercert.pem

smtp-auth-command=/var/qmail/bin/smtp_auth /var/qmail/bin/true /var/qmail/bin/cmd5checkpw /bin/true
smtp-auth-level=ondemand-encrypted

idle-timeout-secs=100
connection-timeout-secs=720
graylist-level=always-create-dir
graylist-dir=/var/qmail/spamdyke/greylist
graylist-min-secs=300
graylist-max-secs=1814400

sender-blacklist-file=/var/qmail/spamdyke/blacklist_senders
header-blacklist-file=/var/qmail/spamdyke/blacklist_headers

recipient-blacklist-file=/var/qmail/spamdyke/blacklist_recipients
ip-in-rdns-keyword-blacklist-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
recipient-whitelist-file=/var/qmail/spamdyke/whitelist_recipient
sender-whitelist-file=/var/qmail/spamdyke/whitelist_sender
ip-in-rdns-keyword-whitelist-file=/var/qmail/spamdyke/whitelist_ip-in-rdns-keyword
greeting-delay-secs=5

dns-blacklist-entry=ix.dnsbl.manitu.net
dns-blacklist-entry=zen.spamhaus.org
dns-blacklist-entry=list.dsbl.org
dns-blacklist-entry=zombie.dnsbl.sorbs.net
dns-blacklist-entry=dul.dnsbl.sorbs.net
dns-blacklist-entry=bogons.cymru.com

reject-missing-sender-mx
reject-empty-rdns
reject-unresolvable-rdns
reject-ip-in-cc-rdns

Zusätzlich müssen einige Verzeichnisse und Dateien angelegt werden, auf die spamdyke zurückgreift.

Code: Alles auswählen

```
mkdir -p /var/qmail/spamdyke/greylist
 touch /var/qmail/spamdyke/blacklist_ip /var/qmail/spamdyke/blacklist_recipients \
  /var/qmail/spamdyke/whitelist_ip /var/qmail/spamdyke/blacklist_keywords \
  /var/qmail/spamdyke/whitelist_recipient /var/qmail/spamdyke/whitelist_sender \
  /var/qmail/spamdyke/whitelist_ip-in-rdns-keyword \
```

```
 /var/qmail/spamdyke/blacklist_senders /var/qmail/spamdyke/whitelist_rdns \
/var/qmail/spamdyke/blacklist_headers
```

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

Im letzten Schritt muss die Einbindung von qmail über den xinetd bearbeitet werden, so dass spamdyke vor qmail-smtpd ausgeführt wird.
Dazu werden die Dateien /etc/xinetd.d/smtp_psa und /etc/xinetd.d/smtps_psa bearbeitet:

Code: Alles auswählen

```
# /etc/xinetd.d/smtp_psa
 service smtp
 {
  socket_type = stream
  protocol = tcp
  wait = no
  disable = no
  user = root
  instances = UNLIMITED
  env = SMTPAUTH=1 POPLOCK_TIME=20
  server = /var/qmail/bin/tcp-env
  server_args = -Rt0 /var/qmail/bin/relaylock /usr/local/bin/spamdyke -f /etc/spamdyke.conf
/var/qmail/bin/qmail-smtpd /var/qmail/bin/smtp_auth /var/qmail/bin/true /var/qmail/bin/cmd5checkpw
/var/qmail/bin/true
 }
```

Code: Alles auswählen

```
# /etc/xinetd.d/smtps_psa
 service smtps
 {
  socket_type = stream
  protocol = tcp
  wait = no
  disable = no
  user = root
  instances = UNLIMITED
  env = SMTPAUTH=1 POPLOCK_TIME=20
  server = /var/qmail/bin/tcp-env
  server_args = -Rt0 /var/qmail/bin/relaylock /usr/local/bin/spamdyke -f /etc/spamdyke.conf
/var/qmail/bin/qmail-smtpd /var/qmail/bin/smtp_auth /var/qmail/bin/true /var/qmail/bin/cmd5checkpw
/var/qmail/bin/true
 }
```

Nach der Änderung muss der xinetd mit dem Kommando /etc/init.d/xinetd restart neugestartet werden. Weitere Schritte sind nicht notwendig.

Vor der Inbetriebnahme sollte aber auf jeden Fall überprüft werden, ob die in der Konfigurationsdatei /etc/spamdyke.conf
vorgenommenen Einträge für den jeweiligen Server sinnvoll sind. Insbesondere die eingetragenen DNSBL sollten überprüft werden.
Wenn deren Nutzung nicht gewünscht ist, müssen die entsprechenden Einträge entfernt oder auskommentiert werden.

Datenbank mit phpmyadmin anlegen:

```
CREATE TABLE `spamdyke_log_table` (
 `id` bigint(7) NOT NULL auto_increment,
```

```
 `time` timestamp NOT NULL default CURRENT_TIMESTAMP,
 `reason` varchar(20) character set utf8 NOT NULL,
 `from` varchar(50) character set utf8 NOT NULL,
 `to` varchar(50) character set utf8 NOT NULL,
 `ip` varchar(15) character set utf8 NOT NULL,
 `rdns` varchar(50) character set utf8 NOT NULL,
 `auth` varchar(25) character set utf8 NOT NULL,
 PRIMARY KEY (`id`),
 KEY `time` (`time`),
 KEY `reason` (`reason`,`from`,`to`,`ip`,`rdns`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

Wartung des Datenbestands (Greylisting)
spamdyke verwaltet die Einträge für das Greylisting nicht selbst. Aufräumarbeiten müssen also periodisch durch einen Cronjob erledigt werden.
Dazu kopieren wir das Script einfach in das richtige Verzeichniss:

```
cd..
```

```
cp -p ./cron/spamdyke-mysql-cleanup /etc/cron.daily/.
```

Das Script im Editor öffnen und anpassen:

```
use constant DBD => 'DBI:mysql:spamdyke:localhost:3306';
use constant DBUSER => 'spamdyke';
use constant DBPASS => 'spamdyke';
```

Nun müssen wir den Wrapper vom Spamdyke Control Panel noch austauschen. Die zip Datei in das spamdyke Verzeichniss entpacken.

Wer keine tägliche Email erhalten möchte, schreibt zusätzlich ein exit; nach dem disconnect:

```
$dbh->disconnect;

exit;
```

Plesk9 Wrapper:

```
gcc wrapper.c -o wrapper
 strip wrapper
```

Nachdem das erledigt ist, tue folgendes:

```
chmod 4755 wrapper
 chown root.root wrapper
```

Bei Debian 6.0 wird nach der Installation eine Fehlermeldung angezeigt. Spamdyke wurde nicht installiert oder die /etc/spamdyke.conf wurde nicht gefunden. Kontrolliere unter /bin/sh den Symbolischen Link. Dieser sollte nicht auf /bin/dash sondern auf /bin/bash verlinkt sein.

Führe folgendes Komando aus:

ln -sf /bin/bash /bin/sh

Weiterführende Informationen
http://www.spamdyke.org/documentation/README.html
http://www.spamdyke.org/documentation/FAQ.html

Eindeutige ID: #1062
Verfasser: Michael Stender
Letzte Änderung: 2012-03-09 04:49