Dosenfleisch & Schädlinge in der Mailbox

SPAMs - den unerwünschten Werbe-E-Mails, die sich täglich zigfach in unseren Mailboxen wieder finden, geht's in diesem WCM Linuxbox-Workshop an den Kragen. Wie Sie der Werbeflut gleich zu Beginn Ihrer Online-Tätigkeit einen Riegel vorschieben oder wie Sie einer bereits begonnen Werbeflut Herr werden - hier steht's geschrieben. Außerdem beugen wir der permanenten Immunschwäche unserer Windows-Clients vor, indem wir Virenscanner in den Mailserver integrieren.

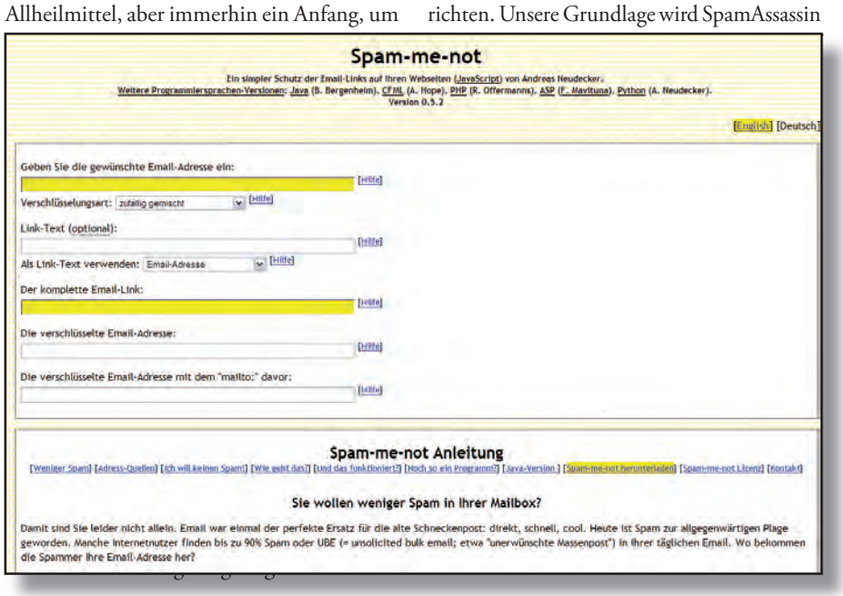
von Martin Müller

Doch wie kommen nun eigentlich die Spammer, also jene, die solche unerwünschten E-Mails verbreiten, zu den E-Mail Adressen? Nun, da gibt es die verschiedensten Möglichkeiten. Zum Beispiel durch spezielle Suchmaschinen, die das Internet durchforsten und E-Mail-Adressen aus den Webseiten filtern. Wenn Sie auf Ihrer Homepage im Kontakt-Bereich einen mailto:-Link haben, ist Ihre Adresse mit großer Wahrscheinlichkeit schon in einer SPAM-Datenbank. Nun können Sie Ihre E-Mail-Adresse entweder mit einem JavaScript schützen, oder in ASCII-Code umsetzen. Das Wort Test sieht codiert so aus: #116;es&#116. Ein Tool das Ihnen die Umschlüsselung nach einer Tabelle abnimmt, finden Sie unter dieser Adresse: http://zapyon.de/spam-me-not/index.de.html. Das ist zwar kein Allheilmittel, aber immerhin ein Anfang, um Wort in Großbuchstaben beim Adressieren entfernen.

Eine weitere listige Art Ihnen Müll in die Mailbox zu stecken, ist der Versand an Kundennummer@provider.at. Oft enthalten die E-Mail-Zugangsdaten für Ihren Provider auch Ihre Kundennummer. Ihr selbst eingerichtetes Alias IhrWunschname@provider.at verweist dann auf diese Mailbox. Es ist für Spammer daher nahe liegend, eine Mailflut an 1@provider.at bis 9999999999@provider.at loszulassen. Gegen so eine Attacke können Sie sich nur mit einem professionellen AntiSPAM-System zur Wehr setzen welches wir hier noch erarbeiten werden.

SPAM-Abwehr für alle E-Mail-Konten

Idealer Weise lassen wir unsere Box die SPAM-Abwehr für alle E-Mail-Konten verrichten. Unsere Grundlage wird SpamAssassin



■ Kurzinfo

Hallo zu einem weiteren Teil der WCM Linux-Box. Der Begriff „SPAM" hat eigentlich gar nichts mit E-Mails zu tun. Er bezeichnet eine spezielle Sorte britischen Dosenfleischs (engl. Ham) das in einem Monty Pythons-Sketch so oft unerwünscht vorkam, dass ein normales Anhören des Sketches nicht mehr möglich war. Ganz so wie die Arbeit am Rechner, wenn nur jede zehnte Nachricht eine „richtige" E-Mail (Ham) ist und man mehr Zeit mit dem Löschen von Werbung (SPAM) verbringt, als mit der Bearbeitung von Nachrichten.

apt-get install amavisd-new spamassassin wird eine Reihe von Applikationen und Bibliotheken installiert, außerdem benötigen wir auf unserer Linux-Box noch einige Dekomprimierprogramme. Damit wird AMaViS in die Lage versetzt auch gepackte Anhänge zu scannen (apt-get install arj zoo lzop zip unzip unzoo bzip2 unalz tar libio-socket-ssl-perl apt-). Und zuletzt müssen auch noch Viren-Scanner auf die Maschine. Wir verwenden zum Einen den gänzlichen freien Scanner clamav (apt-get install clamav-getfiles clamav clamav-daemon clamav-testfiles apt-get clamav-freshclam ca-certificates libcurl3-gssapi). Bei der Installation der Stammzertifikate (CA-Certificate) wählen wir die Option nachfragen und für clamav-freshcalm müssen Sie die richtige Antwort selbst entscheiden. Daemon ist richtig, wenn Sie über eine Standleitung verfügen, ifup.d müssen Sie wählen wenn Sie die Internetverbindung zum Beispiel über pppoe herstellen. Der nächstgelegene Spiegelserver für die Virendefinitionen ist db.at.clamav.net, und wenn Sie die Box nach unserem Beispiel im ersten Workshopteil ans Internet gebracht haben, dann existiert auch kein Proxy. Außerdem lassen wir uns über Updates verständigen.

In der Datei /etc/clamav/freshclam.conf können Sie nun das Updateintervall von clamav nach eigenen Wüschen anpassen. Bei der Installation ist es auf vierundzwanzig Checks am Tag eingestellt. Schnelle Kopfrechner haben es sofort bemerkt: Es wird jede Stunde nach Updates gesucht.

Zum Zweiten verwenden wir den ausschließlich für private Anwendungen kostenlosen f-prot. Wird der Server gewerbsmäßig genutzt, steht er also in einer Firma, müssen Sie eine Lizenz für f-prot erwerben (http://www.fprot.org). Sie müssen diesen zweiten Virenwächter aber nicht installieren, er dient uns als Fallback, sollte der erste einmal versagen.

Wechseln Sie in das Verzeichnis /usr/src/ und holen Sie sich das f-prot-Paket (wget http://www.fprot.org/pub/fp-linux-ws.deb). Danach installieren Sie es mit dpkg -i fp-linux-ws.deb. Während der Installation werden sogleich die Virendefinitionen für f-prot auf den letzten Stand gebracht.

Wir legen einen neuen Eintrag in /etc/crontab an (0 4,8,12,16,24 * * * /usr/local/f-prot/tools/check-updates.pl -cron). Diese Zeile besagt, dass jeden Tag um Punkt vier, acht, zwölf, sechzehn und vierundzwanzig Uhr die Virendefinitionen von f-prot erneuert werden.

Jetzt beginnen wir mit der Konfiguration von amavisd. Dies geschieht in der umfangreichen Datei /etc/amavis/amavisd.conf die in Sektionen eingeteilt ist. In der ersten Sektion nehmen wir Einstellungen zur generellen Arbeit von AMaViS vor. In Zeile 68 finden Sie die Option $mydomain bei der Sie die Domain für die Sie Mails annehmen eintragen. Die Anweisung @bypass_spam_checks_acl in Zeile 161 setzen Sie durch ein vorangestelltes Rautezeichen (#) außer Kraft. Machen Sie das nicht, werden Nachrichten nicht auf SPAM geprüft.

In Sektion III stellen wir der Zeile 278 $DO_SYSLOG ebenfalls ein Kommentarzeichen voran. Andernfalls wird /var/log/syslog von AMaViS-Einträgen überschwemmt. Durch das Kommentarzeichen werden die Log-Einträge in /var/log/amavis.log abgelegt.

Wir beenden vorerst die Konfiguration und versuchen ein telnet localhost 10024. Am Port 10024 sollte sich AMaViS mit ESMTP amavisd-new service ready zum Dienst melden. Beenden Sie telnet durch Eingabe von QUIT.

Postfix muss mitspielen

Nun müssen wir Postfix eine neue Transportmethode beibringen. Postfix soll die E-Mail vom einliefernden Mailserver übernehmen, an AMaVis zur Kontrolle übergeben (Port 10024), sie nach der Kontrolle vom Port 10025 entgegennehmen und weiter zustellen. Dazu ist ein kleiner Eingriff in /etc/postfix/master.cf notwendig. Fügen Sie nach der ersten Zeile die mit smtp beginnt (Zeile 81) eine weitere Zeile, deren Inhalt Sie aus dem Kasten Erweiterung von Postfix entnehmen, ein. Am Ende der Datei brauchen wir weitere Einträge die Sie ebenfalls dem Kasten Erweiterung von Postfix entnehmen. Die leeren Einträge, die mit -o beginnen, sind nötig, um dem Standard zu entsprechen. Bitte lassen Sie diese nicht weg.

Nun weisen wir Postfix in der Datei /etc/postfix/main.cf an, die Mail zur Inhaltsprüfung an den Port 10024 zu übergeben. Dies geschieht durch den Eintrag content_filter = smtp-amavis:[127.0.0.1]:10024. Starten Sie Postfix mit /etc/init.d/posftix restart neu und prüfen Sie mit telnet ob sich Postfix auch am Port 10025 meldet. Wenn nicht, vergleichen Sie Ihre Eingaben in der master.cf mit unseren Vorgaben. Postfix ist hier sehr heikel! Bei Fehlern achten Sie auf Einträge in /var/log/syslog.

Bis jetzt haben wir E-Mails zwar aus Postfix zur Prüfung herausgenommen, wer prüfen soll, haben wir aber noch nicht festgelegt. Also rein in /etc/amavis/amvisd.conf und hin zur Zeile 1248, in der f-prot noch auskommentiert ist. Entfernen Sie alle Rautezeichen bis hin zur Zeile 1256, um nun beide Scanner aktiv werden zu lassen.

Zur ersten Prüfung wird ClamAV heran gezogen, wenn dieser negativ bescheidet, wird die Nachricht an f-prot übergeben um sie nochmals zu checken. Erst wenn auch f-prot grünes Licht gibt, wird die Mail an Postfix zur Zustellung weiter gegeben.

Jetzt legen wir noch fest, was mit infizierten E-Mails passieren soll. Gehen Sie zur Zeile 399. Dort haben Sie die Möglichkeit, bei $final_virus_destiny die Schlussaktion einzustellen. D_REJECT gibt dem einliefernden Mailserver eine Fehlermeldung zurück, wenn die E-Mail nicht zugestellt werden konnte, der Empfänger merkt nichts davon, dass er einen Virus bekommen hätte. D_BOUNCE arbeitet ähnlich, allerdings generiert AMaViS eine Fehler-E-Mail die der Absender zugesendet bekommt, der Empfänger wird nicht benachrichtigt. Von dieser Option raten wir dringend ab, da die meisten Viren-E-Mails mit einem gefälschten Absender versendet werden. D_DISCARD verwirft die Mail vollständig, weder Absender noch Empfänger wissen von der Löschung - sehr gefährlich und sogar laut Gesetz verboten! Nur der tatsächliche Empfänger darf Nachrichten an ihn löschen. D_PASS schließlich stellt die Nachricht trotz Infizierung zu.

Bei allen Lösungen, außer bei D_PASS, werden Kopien der Nachrichten in /vor/lieb/amavis/virusmails gespeichert. Wir empfehlen dieses Verzeichnis regelmäßig zu prüfen. Sie können die enthaltenen Nachrichten

```
<script type="text/javascript">
<!--
var jsvorne = „max.muster";
var jshinten = „wcm.at";
document.write(,\<a href=\"mailto:' + jsvorne + ,@' +
jshinten + ,">');
document.write(xname + ,@' + xendung + ,</a>');
//-->
</script>
```

```
#/etc/postfix/master.cf
Abschnitt 1 - unter dem Eintrag für smtp (Zeile 81)
127.0.0.1:10025  inet   n - n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o receive_override_options=no_unknown_recipient_
   checks,no_header_body_checks
-o smtpd_bin_address=127.0.0.1

Abschnitt 2 - ans Ende der Datei
smtp-amavis unix - - n - 2 smtp
-o smtp_data_done_timeout=1800
-o disable_dns_lookups=yes
-o smtp_send_xforward_command=yes
```

```
#/etc/spamassassin/local.cf
# Die Zeichenfolge *****SPAM***** jeder SPAM hinzufügen

rewrite_subject 1
subject_tag *****SPAM*****
add_header all autolearn _AUTOLEARN_

# Den Schwellwert ab dem die
# Nachricht als SPAM klassifiziert wird

 required_score 5.0
#   Verwende Bayes

use_bayes 1
bayes_path /var/lib/amavis/.spamassassin/bayes_seen

#   Bayes lernt automatisch
 bayes_auto_learn 1
 bayes_auto_learn_threshold_nospam 0.1
 bayes_auto_learn_threshold_spam 8.5

# Einige Headerbestandteile ignorieren,
# die den Bayes-Prozess verwirren könnten
 bayes_ignore_header X-Bogosity
 bayes_ignore_header X-Spam-Flag
 bayes_ignore_header X-Spam-Status

#  Vipuls Razor verwenden
use_razor2 1

#Pfad zu Vipuls Razors Konfigurationsdatei
razor_config /etc/razor/razor-agent.conf

# Pyzor verwenden
use_pyzor 1

# in gescannten mails den header modifizieren
add_header all Pyzor _PYZOR_

# Use DCC-Network
use_dcc 1
dcc_timeout 7
add_header all DCC _DCCB_: _DCCR_

--- Abschnitt für die Crontab ---

#/etc/cron.horly/sa-learn
#!/bin/bash -e
SADIR=/var/lib/amavis/.spamassassin
DBPATH=/var/lib/amavis/.spamassassin/bayes
SPAMFOLDERS="\
  /var/spool/maildir/max.muster/.LERNEN.SPAM/cur \
  /var/spool/maildir/anderer.mailer/.LERNEN.SPAM/cur \
        "
HAMFOLDERS="\
 /var/spool/maildir/max.muster/.LERNEN.HAM/cur/ \
        "
for spamfolder in $SPAMFOLDERS ; do \
  echo Learning spam from $spamfolder ; \
   nice sa-learn --spam --showdots --dbpath $DBPATH
   $spamfolder
done

for hamfolder in $HAMFOLDERS ; do \
        echo Learning ham from $hamfolder ; \
        nice sa-learn --ham --showdots --dbpath $DBPATH
$hamfolder
done
chown -R amavis:amavis $SADIR
```

einfach durch den Befehl less DieNachricht lesen. Das Verzeichnis lässt sich auch verlegen, die Option $QUARANTINEDIR in Zeile 536 ist dafür verantwortlich. Im Falle einer Verlegung, vergeben Sie bitte die entsprechenden Rechte: chown amavis: amavis IhrNeuesVerzeichnis. Verlockend ist die Möglichkeit, die Nachrichten in ein Verzeichnis im Fileserver-Bereich zu legen. Somit haben Sie auch direkten Dateizugriff auf die Nachrichten. Beachten Sie allerdings, dass dies den Virenfilter ad absurdum führt, da die Nachrichten ja jetzt auch von unbedarften Anwendern gelesen werden können - und sie dadurch deren Rechner gegebenenfalls infizieren.

Gefahr gebannt

Wenn Sie sich dazu entschließen, die infizierte Nachricht nicht zuzustellen, (was sinnvoll ist) können Sie sich statt der infizierten Nachricht eine Benachrichtigungs-E-Mail zusenden lassen. Entfernen Sie dazu das Kommentarzeichen in Zeile 442 $warnvirusrecip.

Dieselben Möglichkeiten des Zustellverhaltens haben Sie auch für $final_banned_destiny, $final_spam_destiny und $final_bad_header_destiny. banned regelt das Verhalten für E-Mails mit Anhängen die Datei-Endungen wie .exe enthalten. Welche

Dateien Sie filtern wollen, geben Sie in Zeile 687 an. spam_destiny bezieht sich auf erkannten SPAM, den wir später noch ausführlicher behandeln werden und bad_header betrifft Nachrichten mit nicht konformem Nachrichtenkopf. Den Aufbau eines E-Mail-Headers können Sie gleich bei einer Testmail lesen.

Starten Sie Postfix neu und senden Sie eine Test-E-Mail an einen Account, der auf Ihrer Linux-Box gehostet ist. Lassen Sie sich die E-Mail im Quelltext anzeigen, bei Thunderbird ist dies die Tastenkombination STRG+U, und suchen Sie nach der Zeile X-Virus-Scanned: IhreDomain.org. Siehe da, der Scanner ist aktiv.

Kommen wir nun zur SPAM-Bekämpfung. Wie schon erwähnt arbeitet Spamassassin mit verschiedenen Tests, die je nach Ergebnis so genannte Scores vergeben. Diese Scores können positive oder negative Werte sein, je höher eine Nachricht am Ende bewertet ist, desto wahrscheinlicher ist sie SPAM. Ab einem gewissen Schwellwert wird die Nachricht auf Wunsch ausgeschieden.

Spamkiller

Wir brauchen die Pakete spamassassin razor pyzor. Gleich zu Beginn der Konfiguration editieren wir erst mal /etc/default/spamassassin, in der wir den Wert ENABLED auf 1 setzen. Ohne diese Änderung startet Spamassassin nicht. Nun ist wieder /etc/amavis/amavisd.conf an der Reihe. Wir hüpfen zur Zeile 1121, in der wir den $sa_tag_level_deflt auf -1.000 setzen. Somit wird jeder E-Mail, die bewertet wird, ein X-SPAM-LEVEL-Feld hinzugefügt - und nicht nur wenn die Mail für Spamassassin SPAM ist. Ein sicheres Zeichen dafür, dass die Nachricht auch durch die Filter gegangen ist.

In der nächsten Zeile finden wir $sa_tag2_level_deflt welchen wir auf 5.0 reduzieren. Ab dem Scorewert fünf wird die Mail als SPAM klassifiziert, und entsprechend der Policy in $final_spam_destiny (Zeile 401) ausgeschieden. Auch hier gilt wieder, dass die Option D_BOUNCE ein Schuss ins Blaue ist, da auch Werbe-E-Mails meist einen gefälschten Absender haben und die Fehlernachricht somit einen völlig Unbeteiligten trifft.

In Zeile 1005 finden Sie eine gute Methode, SPAMS das Leben zu verkürzen. Wenn Sie den Wert bei $sa-local_test_only auf 0setzen, dann vergleicht Spamassassin die IP-Adressen jedes am Auslieferungsprozess beteiligten Mailservers, mit den Eintragungen in den SPAM-Blacklists. Gibt es Übereinstimmungen, erhöht dies den SPAM-Score.

Spamassassin in der Grundkonfiguration ist noch nicht sehr mächtig. Wir müssen erst seinen Bayes-Filter einschalten und trainieren. Bayes ist eine mathematische Analyse (Wahrscheinlichkeitsrechnung) der E-Mai,l nach der sie anschließend prozentuell (0 bis 99%) als SPAM bewertet wird.

Den Bayes-Filter aktivieren wir in der /etc/spamassassin/local.cf. Dort fügen wir einige Zeilen beginnend mit use_bayes 1 ein. Die weiteren Zeilen entnehmen Sie bitte dem Kasten „Spamassassin aufgemotzt“. Damit der Filter effektiv arbeitet, muss er trainiert werden. Der Filter kann sich aber auch selbst trainieren. Dazu gibt es zwei Werte, die wir beeinflussen können. Der bayes_autolearn_threshold_nospam-Wert wird so gering wie möglich gehalten, da wir nur E-Mails als Ham bezeichnen wollen, die auch mit Sicherheit kein SPAM sind. Den Wert bayes_autolearn_threshold_spam allerdings setzen wir hingegen relativ hoch an, da nur sicherer SPAM automatisch als SPAM gelernt werden soll.

Wir setzen voraus, dass sie Ihr Mailkonto über das IMAP-Protokoll ansprechen. Erstellen Sie in Ihrem Mailclient ein Verzeichnis unterhalb des Posteingangs, dass Sie mit LERNEN bezeichnen. In diesem LERNEN-Verzeichnis erstellen Sie wieder zwei Ordner, einer wird mit SPAM betitelt, der andere mit HAM. Diese Verzeichnisse brauchen wir, um den Bayesfilter händisch zu trainieren. Wenn Sie Nachrichten empfangen, die durch den SPAM-Filter gerutscht sind, verschieben Sie diese in SPAM. Nachrichten die definitiv Ham sind, legen Sie nachdem Sie sie nicht mehr brauchen, in den HAM-Ordner. Wir definieren ein Cronscript, das nun stündlich die beiden Ordner durchforstet und von den Nachrichten lernt.

Legen Sie dieses Cronscript in /etc/crontab/ unter dem Namen sa-learn ab und machen Sie es ausführbar (chmod a+x /etc/cron.hourly/sa-learn). Das Script finden Sie im Kasten „Spamassassin aufgemotzt“,
- Abschnitt Crontab.

Beachten Sie, dass sie nun die globale SPAM-Datenbanktrainieren. Angenommen Benutzer A findet, dass E-Mails von E-Mailer Z für Ihn SPAM sind und legt sie in seinen SPAM-Ordner. Benutzer B empfindet die Nachrichten vom User Z nicht als SPAM und will Nachrichten vom E-Mailer Z empfangen. Die globale SPAM-Datenbank wird aber nachdem sie genügend Z-SPAMS gelernt hat, die Nachrichten von Z eliminieren. In den SPAM-Ordner dürfen also nur Nachrichten die tatsächlich SPAM sind.

Wen anderen fragen

Eine weitere Erschwernis für Spammer besteht darin, dass wir bekannte SPAMs mit den zuzustellenden Nachrichten vergleichen. Das erledigen die Programme razor2, pyzor und dcc. razor2 vergleicht die Quersumme einer E-Mail mit der SPAM-Datenbank, pyzor und dcc zählen nur die Häufigkeit von E-Mails. Je häufiger ein E-Mail mit demselben Inhalt versendet wird, desto höher ist die Wahrscheinlichkeit dass es sich um SPAM handelt.

Um razor2 benützen zu können, müssen wir ein kostenloses Konto am razor2-Server einrichten. Wir wechseln mit su amavis zum Benutzer amavis und legen durch razor-admin -create das Konfigurationsverzeichnis an. Der Benutzerwechsel ist notwendig, weil AMaVis und razor2 unter demselben User laufen müssen. Danach melden wir uns am razor2-Server an (razor-admin -register) und ermitteln durch razor-admin -discover den nächstgelegenen razor2-Server. Wechseln Sie zurück zum User root (su root), editieren Sie /etc/spamassassin/local.cf und fügen Sie eine Zeile use_razor2 1 hinzu.

Der nächste im Bunde wäre pyzor. pyzor basiert auf der Programmiersprache python, welche deshalb auch auf unserer WCM-Box installiert sein muss. Es ist sehr einfach pyzor einzubinden, in die local.cf muss lediglich add_pyzor 1 eingetragen werden. Fertig, pyzor ist einsatzbereit.

Das Distributed Checksum Clearinghouse, kurz DCC, rundet unseren SPAM-Killer ab. Es vergleicht die Checksummen von E-Mails und kann diese auch als SPAM einstufen wenn die Checksumme von registrierten SPAMs gegenüber den Prüflingen in geringen

Teilen abweichen. Dies kann zum Beispiel bei personalisierten Massenmails der Fall sein. apt-get install dcc-client installiert den Client und die Basis von DCC,

Fehlermeldungen bezüglich fehlender User brauchen Sie nicht stören - das Installationsscript bessert abschließend automatisch nach.

Dass ein Eintrag use_dcc 1 in der local.cf notwendig ist, braucht an dieser Stelle fast nicht mehr erwähnt werden.

Fine-Tuning

Um die Treffer der Scores für den Bayes-Filter zu erhöhen, fügen wir in der Datei /usr/share/spamassassin/20_drugs.cf hinzu. Gehen Sie in Zeile 87 und erweitern Sie die Regelkette innerhalb der Klammer um |pharmacy. Der Strich am Anfang des Wortes pharmacy ist kein Schrägstrich oder L, sondern die so genannte Pipe |. Auf den meisten Tastaturen finden Sie die Pipe auf ALT+>.

Da wir Europäer eher selten Nachrichten entziffern können, die einen Zeichensatz aus [illegible]en verwenden, wollen wir solche Mails gleich mal höher bewerten als Nachrichten die einen westlichen Zeichensatz verwenden. Dazu braucht´s in der local.cf eine Zeile mit ok_locales en und einer weiteren Zeile score CHARSET_FARAWAY 3.5. Jetzt werden Nachrichten die einen anderen Zeichensatz verwenden automatisch um 3.5 Punkte höher eingestuft.

Die Konfiguration ist abgeschlossen, Sie müssen nun spamassassin, amavis und postfix in dieser Reihenfolge neu starten. Der Mailserver ist nun einsatzbereit und sie können die ersten Mails durch die Filter schleusen.

Eine recht brauchbare Methode um SPAM zu filtern und trotzdem einen Überblick zu haben, ob nicht vielleicht doch HAM dabei ist, ist dass Sie $final_spam_destiny auf D_PASS setzen. Jede E-Mail, und sei deren Score noch so hoch, wird durchgelassen, der Betreff der Nachricht die den SPAM-Level überschreitet jedoch mit ***SPAM*** gekennzeichnet. Definieren Sie in Ihrem MUA (MailUserAgent: z.B. Thunderbird oder Outlook Express) einen Filter, der sämtliche Nachrichten deren Betreff mit ***SPAM*** beginnt in einen Ordner verschiebt. Somit haben Sie auch Zugriff auf fälschlicher Weise klassifizierte Nachrichten.

Eine wichtige Regel zum Schluss: Sollte trotzdem das eine oder andere SPAM-E-Mail durchdringen, benutzen Sie niemals den Link „Abmelden“ im SPAM. Durch Ihre Antwort erhält der Absender Gewissheit dass sein Müll tatsächlich gelesen wurde und somit eine indirekte Empfangsbestätigung. Für den Absender ist Ihre Adresse im Wert gestiegen, da er sicher sein kann, dass weitere Werbungen auch einen Abnehmer finden. ■