

Filtern von Spam-Mails direkt auf dem Server

Von Lars Witter (Vorstand Mabi)

Marburg, den 18.08.2003

Seit etwa 3 Monaten betreiben wir auf den Mabi-Mail-Servern eine Spamerkennungssoftware, der eingehende E-Mails nach verschiedenen Spam-Kriterien durchsucht und bewertet. Dieser Filter fügt in jeder als Spam erkannten Mail einige, normalerweise nicht sichtbare Zeilen ☀ im Mailheader (Kopfzeile) ein. Diese Einträge im Mailheader können durch Filterregeln, sowohl bereits auf dem Server wie auch im E-Mail-Programm, zur Aussortierung von Spam genutzt werden. Im folgenden die Beschreibung für das Anlegen von Filterregeln direkt auf dem Server

Nähere Informationen zu der Spamerkennungssoftware erhalten Sie unter: <http://www.spamassassin.org/index.html>

☀ Hier mal ein Auszug aus einer als Spam erkannten und markierten E-Mail

```
X-Spam-Flag: YES
X-Spam-Status: Yes, hits=12.5 required=5.0
  tests=HTML_30_40,HTML_FONT_BIG,HTML_FONT_COLOR_RED,HTML_MESSAGE,
  MIME_HTML_NO_CHARSET,MIME_HTML_ONLY,MISSING_MIMEOLE,
  MISSING_OUTLOOK_NAME,NORMAL_HTTP_TO_IP,PENIS_ENLARGE,
  PENIS_ENLARGE2,RATWARE_EGROUPS,RCVD_IN_NJABL,
  RCVD_IN_UNCONFIRMED_DSBL
  version=2.55-hgmdevnull
```

X-Spam-Report: ---- Start SpamAssassin results

```
12.50 points, 5 required; ←
* 4.3 -- Bulk email software fingerprint (eGroups) found in headers
* 1.4 -- BODY: Information on getting a larger penis or breasts
* 1.3 -- BODY: Information on getting a larger penis or breasts (2)
* 0.9 -- BODY: Message is 30% to 40% HTML
* 0.1 -- BODY: HTML font color is red
* 0.1 -- BODY: HTML included in message
* 0.3 -- BODY: FONT Size +2 and up or 3 and up
* 0.8 -- RAW: Message text in HTML without specified charset
* 0.7 -- URI: Uses a dotted-decimal IP address in URL
* 0.9 -- RBL: Received via a relay in dnsbl.njabl.org
[RBL check: found 233.81.233.219.dnsbl.njabl.org., type: 127.0.0.9]
* 0.5 -- RBL: Received via a relay in unconfirmed.dsbl.org
[RBL check: found 233.81.233.219.unconfirmed.dsbl.org.]
* 0.1 -- Message only has text/html MIME parts
* 0.5 -- Message has X-MSMail-Priority, but no X-MimeOLE
* 0.6 -- Message looks like Outlook, but isn't
```

---- End of SpamAssassin results

X-Spam-Level: *****

X-Spam-Checker-Version: SpamAssassin 2.55-hgmdevnull (1.174.2.19-2003-05-19-exp)

Ist die E-Mail womöglich Spam?

Highscore der ermittelten Punkte.

Im folgenden eine Übersicht über die Bewertung der E-Mail.

Ein Spamfilter durchsucht die E-Mails nach bestimmten Kriterien wie z.b.

- Schriftgröße
- Stil (HTML-/Text-E-Mail)
- "verbotene" Worte z.b. Sex, Penis
- Absendeadresse

All diese Kriterien werden wenn sie zustimmen mit Punkten bewerten und am Ende werden alle Punkte addiert.

Wie man an diesem Auszug erkennen kann hat die E-Mail die „volle“ Punktzahl um mehr als das doppelte überschritten.

Mit „volle“ Punktzahl ist die Punktzahl gemeint die man angeben kann, ab wann eine Mail als Spam erkannt wird.

Eine E-Mail, die 4.9 Points erreicht wird nicht als Spam erkannt, erst ab 5 Punkten ist sie laut unserer (und der von Spamassassin) Definition Müll.

Genauere Informationen können unter o.g. Adresse nachgelesen werden.

So, dann wollen wir mal eine Filterregel anlegen.

Der Start, wie gewohnt mail.mabi.de im Browser öffnen und Anmeldedaten eingeben – danach erscheint dieses Fenster

Main Menu

lw

Current Mailbox: Main

Mailbox	Size (bytes)	Message Count	Last Modified
Main	0	0/0	2003-09-18 14:53
Sent	0	0	2003-09-04 12:16
Deleted	0	0	
Archiv	0	0	2003-09-04 12:09
Draft	0	0	2003-04-21 11:53
Spam	1111025	216	2003-09-18 14:32

Current Mailbox: Main

Options

Personal

- [Change Finger Information](#)
- Change Password not allowed**
- [Change Mail Forwarding Information](#)
- [Change User Information](#)
- [Change Vacation Message](#)
- [Change Processing Rules](#)
- [Address Book](#)
- [Manage Mailboxes](#)
- [Auto Response](#)

Administration

- [View Spool Directory](#)
- [Edit News Message](#)
- [Edit Welcome Message](#)
- [View Monitor Access Log](#)
- [View Monitor System Log](#)
- [View IMail Syslog Log](#)
- [View IMail System Log](#)
- [Recent IMail News](#)
- [Virtual Hosts](#)

Eventuell hier - falls ein „+“ vor „Options“ steht - anklicken um die Optionen anzuzeigen

Nun folgt man diesem Link

Hier werden dann die entsprechenden Filter gesetzt oder geändert.

Im neu erscheinenden Dialog auf diese Schaltfläche klicken

Lars - Server Processing Rules

To add a new rule, click on the Add button.

Logoff

Menu

Add

Auf dieser Seite kann nach allem was eine E-Mail hergibt gefiltert und sortiert werden.

Wir wollen Spam filtern, den der Spammassassin als Müll erkannt hat.

Hier wird **Header** ausgewählt, da das zu suchende Kriterium sich im Email-Header befindet.

Eingabe des Kriteriums:
X-Spam-Flag: YES
(So werden Spam-Mail markiert)

Hier stehen mehrere Möglichkeiten zur Auswahl

<new>: legt einen neuen Ordner mit dem unter 4 angegebenen Namen

<delete>: löscht Spam-Mails sofort!

Danach folgt eine Liste der bereits vorhandenen Ordner

Iw - Add a Rule

Logoff
Menu
Add
Help

Send mail when the contains doesn't contain

Search string from file

to the Mailbox

Match Case

Enter a search string in the text box above. Enable the checkbox to allow the search text to come from an external file. The listbox shows a list of the existing rule files. Click on 'Update' to get the contents of selected rule file. The maximum limit for a direct search string (not from an external file) is 255. Search strings more than 255 will be truncated at 255.

Select a mailbox from the list or Enter a new mailbox. Incoming mail will be directed to this mailbox when the rule is asserted. When "<new>" is selected user has to enter a new mailbox name in the textbox. If nothing is entered in the textbox the mailbox name is taken as "new".

Enable this option for a case sensitive match.

IMail Server for Windows NT Web Messaging from Ipswitch, Inc.

Vollständig ausgefüllt sieht die Filterregel so aus.

Erklärung:

Es wird nach einem Kriterium im Header (Nachrichtenkopfeilen) gesucht die mit „X-Spam-Flag: YES“ übereinstimmt.

Sollte eine Mail gefunden werden, so erstelle (falls noch nicht geschehen einen neuen Ordner namens „Spam“) bzw. verschiebe die Mail in den Ordner.

Beachte aber nicht die tatsächliche Schreibweise. Ein „x-spam-flag: yes“ würde genauso gefiltert werden.

Jetzt noch links auf **ADD** und fertig.

IMail Server - Microsoft Internet Explorer

Adresse <http://212.89.202.7/>

Handshake Group Marburg

Lars - Server Processing Rules

To add a new rule, click on the Add button.

Logoff
Menu
Add

Existing Rules

Field	Rule	Value	Sub-Area		
Header	contains	X-Spam-Flag: YES	Spam		Modify Delete

Delete All

[Enter secure mode.](#)

IMail Server for Windows NT Web Messaging from Ipswitch, Inc.

<http://www.mabi.de/info.html> Internet

Wenn alles klar gegangen ist müsste das folgende Fenster so aussehen.

Mit „Modify“ kann man die Regel ändern und mit „Delete“ wieder löschen.

Probieren Sie bitte das Filtern zu Beginn mit dem Verschieben in einen neuen Ordner und prüfen Sie immer wieder ob wichtige Mails versehentlich als Spam markiert wurden und dadurch in dem Spam-Ordner gelandet sind.

Beachten Sie bitte diese Mails verbrauchen ebenfalls Speicherplatz in Ihrer Mailbox!

Die Mails aus dem Extra-Ordner können nicht mit einem POP3-Client abgeholt werden – Dazu müssen Sie in Ihren Email-Client ein IMAP-Konto einrichten oder die Spam-Mails über das Webinterface löschen.

Nach einer positiven Testphase können Sie dann die Regel so ändern, dass die Mails direkt gelöscht werden.

Hilfe zum Einrichten der verschiedenen Kontenarten in Ihrem E-Mail-Client (E-Mail-Programm) entnehmen Sie bitte Ihrem jeweiligen E-Mailprogramm

Diese Anleitung darf nur von Usern des HGM e.V. eingesehen, ausgedruckt und unter diesen verteilt werden - Jegliche Änderung ist untersagt!

© 2003 by Lars Witter (Vorstand Mabi)