Spamfilter

Allgemeines

Auf dem Mailserver laeuft als Filter Amavis, der zur eigentlichen Spamfilterung SpamAssassin und zur Virussuche ClamAV benutzt.

SpamAssassin funktioniert so, dass es Mails nach typischen Kriterien fuer Spam untersucht und pro gefundenem Merkmal eine gewisse Menge (positiver) Punkte vergibt. Fuer typische Kriterien erwuenschter, normaler Mails (Ham) werden ggf. negative Punkte vergeben. Am Ende wird eine Gesamtsumme pro Mail errechnet.

Ueberschreitet diese Summe den Wert 25, lehnt der Mailserver Mails komplett ab. Bleibt der Wert darunter, werden ggf. spezielle Header in die Mail geschrieben. Manuell wurden durch ungluecklicheKombination von Begriffen (verschicken der Spamfilter-Konfiguration per Mail) bisher nur etwa 10 Punkte durch eine regulaere Mail erreicht. Erwuenschte Mails liegen optimalerweise unter 0, koennen aber auch mal knapp darueber liegen.

Spezielle Mail-Header

Eine normale Mail wird vom Spamfilter beispielsweise so markiert:

Ham

```
X-Spam-Flag: NO
X-Spam-Score: -3.261
X-Spam-Status: No, score=-3.261 required=5 tests=[AWL=-0.662,
BAYES_00=-2.599]
        autolearn=ham
```

Eine (erkannte) Spam-Mail kann beispielsweise so markiert sein:

Spam

```
X-Spam-Flag: YES
X-Spam-Score: 26.557
X-Spam-Level: **************************
X-Spam-Status: Yes, score=26.557 required=5 tests=[BAYES_99=4, IXHASH=2.5,
        LOGINHASH=4.5, MISSING_DATE=1.5, MISSING_MID=0.001,
        RCVD_IN_BL_SPAMCOP_NET=1.96, RCVD_IN_PBL=0.905,
        RCVD_IN_SORBS_DUL=0.877, RCVD_IN_XBL=3.033, RCVD_NUMERIC_HELO=2.067,
        RDNS_NONE=0.1, TVD_RCVD_IP=1.931, TVD_RCVD_IP4=3.183] autolearn=spam
```

„X-Spam-Flag“ wird uebrigens ab einem Punktelevel von 5 gesetzt. In „X-Spam-Status“ wird uebrigens

festgehalten, welche Merkmale gefunden wurden.

Wurden Viren oder anderweite unerwuenschte Anhaenge entdeckt, kann wird einer der folgenden Header gesetzt:

Virus

```
X-Amavis-Alert: INFECTED
X-Amavis-Alert: BANNED
```

Wie man leicht sieht, sind die Header „X-Spam-Level“, „X-Spam-Flag“ und „X-Amavis-Alert“ fuer die Filterung am interessantesten.

Filterung

Auf Mailinglisten

Im Webinterface kann man unter „Privacy options…“/„Abo-Regeln und Adreßfilter…“, Unterpunkt „[Spam filters]“/„[Spam-Filter]“ entsprechende Filter bei „header_filter_rules“ anlegen.

Beispiele:

- erkannten Spam und Viren moderieren
  - als Aktion „Hold“/„Zurückhalten“ auswaehlen
  - folgenden Kriterien verwenden:

```
X-Spam-Flag: Yes
X-Amavis-Alert: INFECTED
X-Amavis-Alert: BANNED
```

- Spam mit hohem Level (ab 15 Punkten respektive 15 Sternen) wegwerfen
  - als Aktion „Discard“/„Wegwerfen“ einstellen
    - nicht „Reject“/„Ablehnen“ waehlen, da Spam meist mit gefaelschten Adressen verschickt wird und man somit unbeteiligte Dritte belaestigen wuerde
  - die Wegwerf-Regel sollte vor der Moderations-Regel eingefuegt werden, da die Mails sonst trotzdem moderiert werden muessen
  - folgendes Kriterium verwenden:

```
X-Spam-Level: [*]{15,}
```

Manchmal will man auch eine Maillingliste, die primaer fuer eine geschlossene Benutzergruppe wie Uni-Mailadressen gedacht ist. Dazu kann man folgende Einstellungen taetigen:

- geschlossene Benutzergruppe (jeder mit passender Absenderadresse darf an die Liste schreiben, ohne selbst Mitglied sein zu muessen)
    - „Privacy options…“/„Abo-Regeln und Adreßfilter…“, Unterpunkt „Sender filters“/„Absender-Filter“:
        - „generic_nonmember_action“ entweder auf „Hold“/„Zurückhalten“ (zwecks Moderation) bzw. „Reject“/„Ablehnen“ bzw. „Discard“/„Wegwerfen“ einstellen
        - „accept_these_nonmembers“ einrichten, um alle Absender-Adressen zu erlauben, die „@tu-ilmenau.de“ enthalten:

```
^.*@tu-ilmenau.de
```

Im Client

Je nach E-Mail-Programm sind die Filter auf unterschiedliche Weise einzurichten, und diese Funktion wird auch nicht von allen Programmen unterstuetzt. Wenn nicht, kann man einen separaten Mailfilter wie procmail oder Sieve verwenden. Die Einrichtung von Sieve ist sieve-mailfilter| hier erklärt. Prinzipiell sollte man wie auch bei den Mailinglisten auf die obigen Header filtern.

Alternativ – oder auch in Kombination – kann man die Markierungen des Mailservers auch ignorieren, wenn man ein Programm wie Thunderbird benutzt, das bereits einen eingebauten, eigenen Spamfilter enthaelt.