deutsches forschungsnetz

Forum Mail:
amavis und spamassassin wissen die Antwort

82. DFN-Betriebstagung | 25.03.2025

Andrea Wardzichowski

Zentrale Frage

- Warum wurde eine Mail als Spam erkannt (und hoffentlich in einen Werbe-Ordner abgelegt) oder abgewiesen?

Mailheader

X-Spam-Report:

* **8.0 URIBL_ZRD** Contains a URL listed in the Spamhaus ZRD blocklist
* **[URI: guenstigschnell.nl]**
* **8.0 URIBL_DBL_SPAM** Contains a spam URL listed in the Spamhaus DBL
* blocklist
* **[URI: www.guenstigschnell.nl]**
* -0.0 SPF_PASS SPF: sender matches SPF record
* 0.0 SPF_HELO_NONE SPF: HELO does not publish an SPF Record
* 0.9 BAYES_999 BODY: Bayes spam probability is 99.9 to 100%
* [score: 0.9999]
* 7.0 BAYES_99 BODY: Bayes spam probability is 99 to 100%
* [score: 0.9999]
* 0.0 BT_95 BODY: Test Bayes spam probability is 95 to 99%
* [score: 0.9841]
* **7.0 DFN_PHISH_OK01 Subject is known spam sender**
* 0.9 RCVD_IN_MSPIKE_L4 RBL: Bad reputation (-4)
* [209.141.55.141 **listed in bl.mailspike.net]**
* **1.5 DATE_IN_PAST_06_12 Date: is 6 to 12 hours before Received: date**
* 0.0 HTML_MESSAGE BODY: HTML included in message
* 7.5 BOGO_SPAM Bogofilter detected spam.
* 0.0 BOTE_SPAM Test bogofilter detected spam.
* 0.0 RCVD_IN_MSPIKE_BL Mailspike blocklisted
* -0.0 RPZOR rpz or dbl hit
* -0.0 RPZDBL dbl hit without rpz hit
* -0.0 DMARC_PASS DMARC pass policy

syslog

- Wird zugestreamt (gern mit TLS)
- Der DFN hält die Logs sieben Tage:

Feb 27 11:27:09 mgw6-han amavis[2495806]: (100-1-01) Passed SPAMMY {AcceptedInbound}, 100-1 [209.141.55.141] [209.141.55.141] <FROM> -> <wardzichowski@dfn.de>, Queue-ID: 655102C00C4, Message-ID: <0.0.2F.68F.1DB88BFBC2274DC.0@dating.aasan.com.au>, mail_id: 3oN26QtVXfX5, **Hits: 40.835**, size: 4855, 497 ms, Tests: [BAYES_999=0.9,**BAYES_99=7,BOGO_SPAM=7.5**,BOTE_SPAM=0.01,BT_95=0.01,DATE_IN_PAST_06_12=1.543,DFN_PHISH_OK01=7,DMARC_PASS=-0.01,HTML_MESSAGE=0.001,RCVD_IN_MSPIKE_BL=0.001,RCVD_IN_MSPIKE_L4=0.9,RPZDBL=-0.01,RPZOR=-0.01,SPF_HELO_NONE=0.01,SPF_PASS=-0.01,**URIBL_DBL_SPAM=8,URIBL_ZRD=8**], helo: dating.aasan.com.au, From: "Neue_Nachricht"_<FROM>

syslog (2)

Feb 27 11:27:09 mgw6-han amavis[2495806]: (100-1-01) X-Spam-Report: \n* **8.0 URIBL_ZRD Contains a URL listed in the Spamhaus ZRD blocklist\n* [URI: guenstigschnell.nl]**\n* 8.0 URIBL_DBL_SPAM Contains a spam URL listed in the Spamhaus DBL\n* blocklist\n* [URI: www.guenstigschnell.nl]\n* -0.0 SPF_PASS SPF: sender matches SPF record\n* 0.0 SPF_HELO_NONE SPF: HELO does not publish an SPF Record\n* 0.9 BAYES_999 BODY: Bayes spam probability is 99.9 to 100%\n* [score: 0.9999]\n* 7.0 BAYES_99 BODY: Bayes spam probability is 99 to 100%\n* [score: 0.9999]\n* 0.0 BT_95 BODY: Test Bayes spam probability is 95 to 99%\n* [score: 0.9841]\n* **7.0 DFN_PHISH_OK01 Subject is known spam sender**\n* **0.9 RCVD_IN_MSPIKE_L4 RBL: Bad reputation (-4)\n* [209.141.55.141 listed in bl.mailspike.net**]\n* 1.5 DATE_IN_PAST_06_12 Date: is 6 to 12 hours befo re Received: date\n* 0.0 HTML_MESSAGE BODY: HTML included in message\n* 7.5 BOGO_SPAM Bogofilter detected spam.\n* 0.0 BOTE_SPAM Test bogofilter detected spam.\n* 0.0 RCVD _IN_MSPIKE_BL Mailspike blocklisted\n* -0.0 RPZOR rpz or dbl hit\n* -0.0 RPZDBL dbl hit without rpz hit\n* -0.0 DMARC_PASS DMARC pass policy\n

Feb 27 11:27:09 mgw6-han amavis[2495806]: (100-1-01) Passed SPAMMY {AcceptedInbound}, 100-1 [209.141.55.141] [209.141.55.141] <FROM> -> <wardzichowski@dfn.de>, Queue-ID: 655102C00C4, Message-ID: <0.0.2F.68F.1DB88BFBC2274DC.0@dating.aasan.com.au>, mail_id: 3oN26QtVXfX5, **Hits: 40.835**, size: 4855, 497 ms, Tests: [BAYES_999=0.9,BAYES_99=7,BOGO_SPAM=7.5,BOTE_SPAM=0.01,BT_95=0.01,DATE_IN_PAST_06_12=1.543,DFN_PHISH_OK01=7, DMARC_PASS=-0.01,HTML_MESSAGE=0.001,RCVD_IN_MSPIKE_BL=0.001,RCVD_IN_MSPIKE_L4=0.9,RPZDBL=-0.01,RPZOR=-0.01,SPF_HELO_NONE=0.01,SPF_PASS=-0.01,URIBL_DBL_SPAM=8,URIBL_ZRD=8], helo: dating.aasan.com.au, From: "Neue_Nachricht"_<FROM>

amavisgrep

- Perlscript, geht zweimal durch das Logfile und produziert lesbaren output
- Ähnlich wie im Mailheader aufgebaut
- Summarische Auflistung der Punkte

```
SH_HBL_EMAILS_GMAIL          1.00
FORM_FRAUD_3                 1.69
FREEMAIL_FORGED_REPLYTO      2.10
BAYES_99                     7.00
BOGO_SPAM                    7.50
-----------------
Spam-Score:          21.45
envfrm->to:          <from@from> -> <to@to>
header-frm:          "XXXXXXXXXXXXXX"_<from>
```

spamassassin

- Checks, die mit 0.01 Punkten bewertet werden
- Was soll das?
- „Was wäre wenn“
- Würde der Check mit > 7 Punkten scharf geschaltet, was würde alles wegsortiert bzw. sogar abgelehnt
- Beispiel: was würde bei einer „strengen“ Einstellung SPF „**-all**“ alles hart abgelehnt

=> gut, um neue Checks zu testen

Wieviele Spampunkte auf neue Checks?

- Ausloten mit 0.01 Punkten und syslog auswerten
- Was soll erreicht werden?

  Markierung und Wegsortieren oder

  Ablehnung?

=> Wir beraten gerne!

Fazit und Datenschutzhinweis

- Sie können selber viel im syslog nachsehen
- Wenn Sie die Hotline per Mail kontaktieren,

  seien Sie bitte datenparsam und übermitteln Sie nur das Nötigste
- s.a. https://www.mailsupport.dfn.de/kontakt :

  “Wenn Sie unsere Hotline per E-Mail kontaktieren, überlegen Sie bitte:
  reicht es für Ihre Anfrage aus, From:, To: und Datum/Zeit mitzusenden oder
  brauchen wir die Header (Kopfzeilen) der Mail oder wird die ganze Mail benötigt,
  weil es sich um Fragen zu checks handelt, die den Body der Mail (Text-Teil)
  behandeln? In diesem Fall senden Sie uns die Mail bitte als Attachment zu.“

Haben Sie noch Fragen?

- Kontakt
  - https://www.mailsupport.dfn.de/
  - hotline@mailsupport.dfn.de
  - Telefon: 0049 711 633 14 217