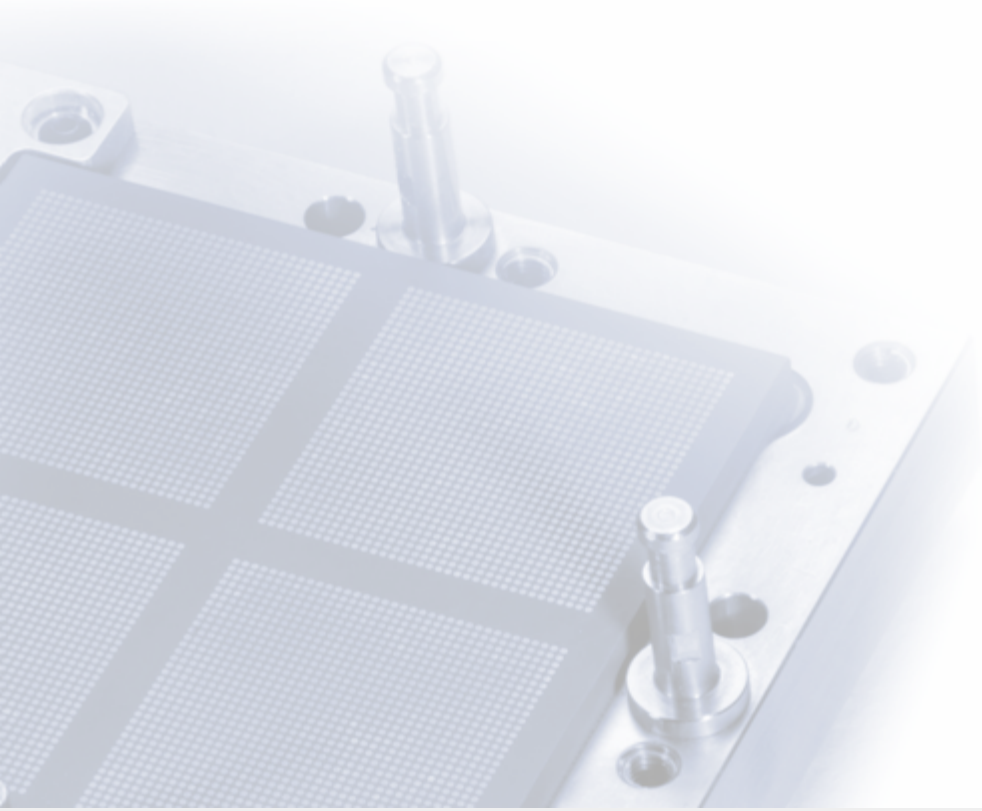
Leibniz Universität Hannover

Neue SPAM- und Virenabwehr

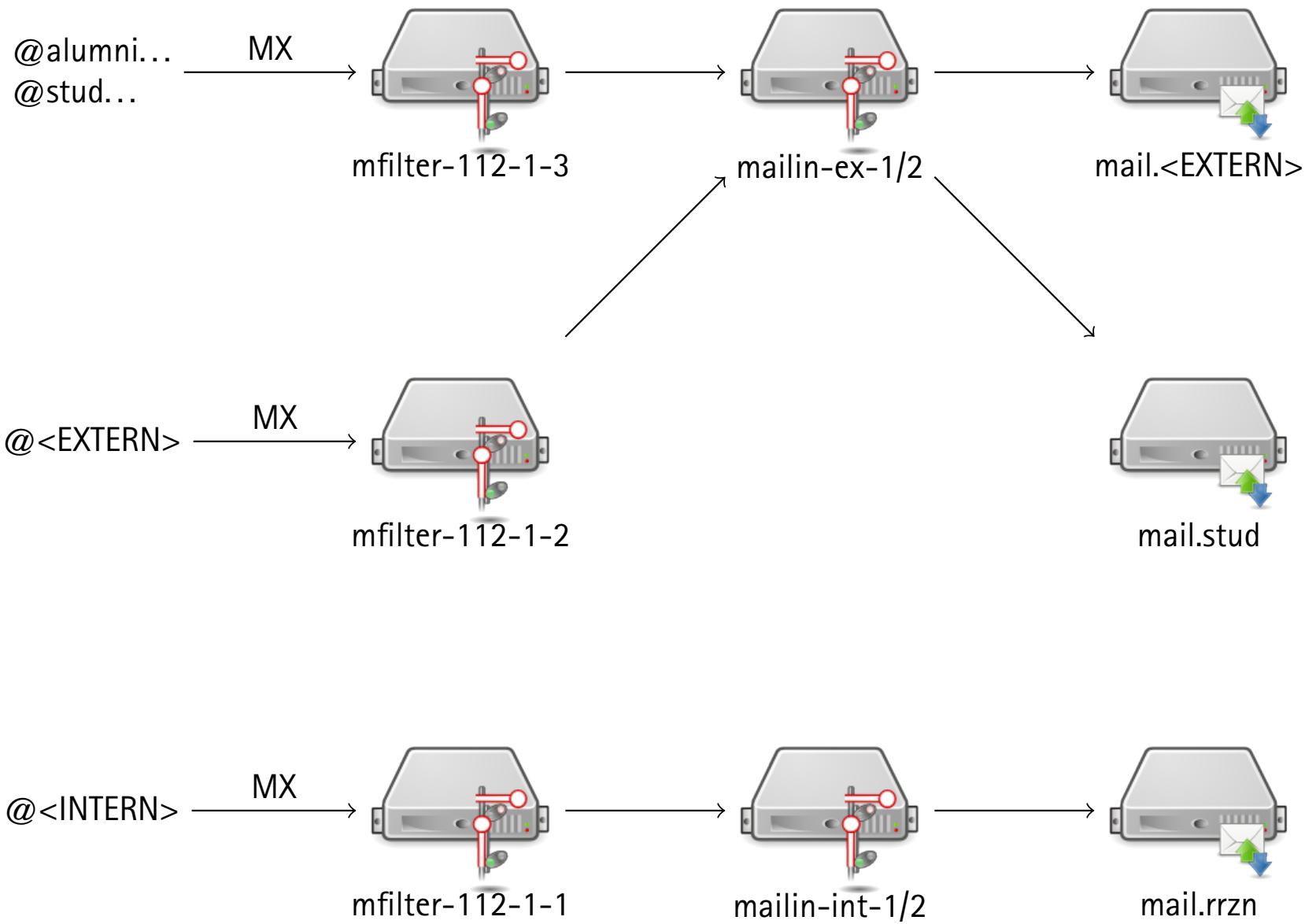
Hergen Harnisch & Mark Heisterkamp
{harnisch,heisterkamp}@rrzn.uni-hannover.de



Leibniz Universität Hannover

Mailsetup DFN → RZ

Mailsetup DFN → RZ



Leibniz Universität Hannover

Mailsetup DFN → RZ

Softwarekomponenten DFN

DNS

User unknown – Postfix Recipient Address Verification

Sortierung auf dem Mailserver

Mailheader – Filter-Policy

Training für die Spamerkennung

Zahlen

Ausblick

Links

Softwarekomponenten DFN

- Relay: Postfix
- Filter-Framework: amavis
- Virenerkennung: ClamAV, Avira, Sophos
- Spamerkennung: spamassassin, bogofilter
- Policyfilter: RBL
  - zen.spamhaus.org
  - dbl.spamhaus.org
  - bl.spameatingmonkey.net
  - fresh10.spameatingmonkey.net
  - ix.dnsbl.manitu.net
  - dsn.rfc-ignorant.org

Leibniz Universität Hannover

Mailsetup DFN → RZ

Softwarekomponenten DFN

DNS

User unknown – Postfix Recipient Address Verification

Sortierung auf dem Mailserver

Mailheader – Filter-Policy

Training für die Spamerkennung

Zahlen

Ausblick

Links

DNS

- DNS und Mail bei uns: nix zu tun
- DNS am Institut, Mail bei uns:

```
institutsdomain.de. IN MX 10 mfilter-112-1-1.mx.srv.dfn.de.
institutsdomain.de. IN MX 10 mfilter-112-1-2.mx.srv.dfn.de.
institutsdomain.de. IN MX 10 mfilter-112-1-3.mx.srv.dfn.de.
```

- DNS und Mail am Institut:

```
institutsdomain.de. IN MX 10 mfilter-112-2-1.mx.srv.dfn.de.
institutsdomain.de. IN MX 10 mfilter-112-2-2.mx.srv.dfn.de.
institutsdomain.de. IN MX 10 mfilter-112-2-3.mx.srv.dfn.de.
```

Leibniz Universität Hannover

User unknown – Postfix Recipient Address Verification

- Die DFN-Relays lernen gültige und ungültige Empfänger durch Testmails. Dementsprechend muss das empfangende Relay bei uns User unknown zurückliefern können.
- Positive Antworten (Empfänger existiert) bleiben 7 Tage im Cache,
- negative Antworten (User unknown) bleiben 30 Minuten im Cache.
- Bei Betrieb eines Mailservers am Institut gilt das ebenfalls, schalten Sie also das 'User unknown'-Feature ein!

Leibniz Universität Hannover

Quarantäne-Ablösung

vorher unter PureMessage

Wer an der Spam-Abwehr teilgenommen hat, hatte die Wahl

- Spam-Mails für 14 Tage in PMX-Quarantäne
- ggf. mit täglicher Digest-Mail

Umstellung auf DFN

- Tagging im Header der Mail durch DFN-Relais
- Aussortierung im Mailaccount als Grundprinzip

Aussortierung

Bei Tagging kann Sortierung eigentlich individuell festgelegt werden:

- Filterskripte auf dem Mailserver
- Filterskripte im Mailclient
- … oder gar nicht

Aussortierung

Bei Tagging kann Sortierung eigentlich individuell festgelegt werden:

- Filterskripte auf dem Mailserver
- Filterskripte im Mailclient
- … oder gar nicht

Standard beim Rechenzentrum

Da auf Mailserver für den Nutzer am einfachsten ist:
Aussortierung in einen extra Ordner, der automatisch gelöscht wird.

- Sieve-Filterregel „LUH-Spamfilter“ sortiert in Ordner „30dTrash“
- Nutzer kann Regel über Webmail aktivieren und deaktivieren
- Ordner „30dTrash“ wird nächtlich von Mail älter als 30 Tage befreit

Ausnahmen & Besonderheiten

Pop3

Bei Pop3 wird nur die INBOX abgerufen, 30dTrash nicht:
„LUH-Spamfilter“ ist dann wie PMX-Spamfilter ohne Digest

⟶ Nutzer wurden in Info-Mail auf Pop3-Problem hingewiesen.

Instituts-Mailserver

Nicht alle Mail-Accounts liegen beim Rechenzentrum:
nachgelagerte Mailserver müssen ggf. Ähnliches implementieren,
alternativ Filterung in Mail-Clients

⟶ Mailserver-Admins wurden gesondert angeschrieben.

Umstellung

Nutzer-Information:

- Nutzer-Information durch Info-Mail
- zudem spezielle Mail in 30dTrash-Ordner
- Ausführliche Webseiten

Sieve-Skripte:

- Sieve-Regel musste über Horde eingefügt werden
- Horde-Web-GUI dafür geskriptet, um nichts kaputt zu machen

Umstellung

Nutzer-Information:

- Nutzer-Information durch Info-Mail
- zudem spezielle Mail in 30dTrash-Ordner
- Ausführliche Webseiten

Sieve-Skripte:

- Sieve-Regel musste über Horde eingefügt werden
- Horde-Web-GUI dafür geskriptet, um nichts kaputt zu machen

Größte Probleme:

- Horde-Bugs erforderten unerwarteten Eingriff in DB, teilweise Regeln vor Umstellung fehlerhaft und daher inaktiv
- MX-Records in fremden DNS-Zonen

Nachfragen & Support

Wir hatten deutlich erhöhten Support befürchtet, blieb aus:

Häufigste Supportanfrage

„Was ist los, ich bekomme kein Spam mehr. Funktioniert alles?“

Nachfragen & Support

Wir hatten deutlich erhöhten Support befürchtet, blieb aus:

Häufigste Supportanfrage

„Was ist los, ich bekomme kein Spam mehr. Funktioniert alles?“

Erwartete Kritik blieb ebenfalls aus:

- kein Wunsch nach Digest geäußert, auch nicht bei Pop-Usern
- keine Angst vor False-Postives, eher andersrum

Generelles zu Sieve-Skripten

Sieve-Regeln werden teilweise unsachgemäß eingesetzt:

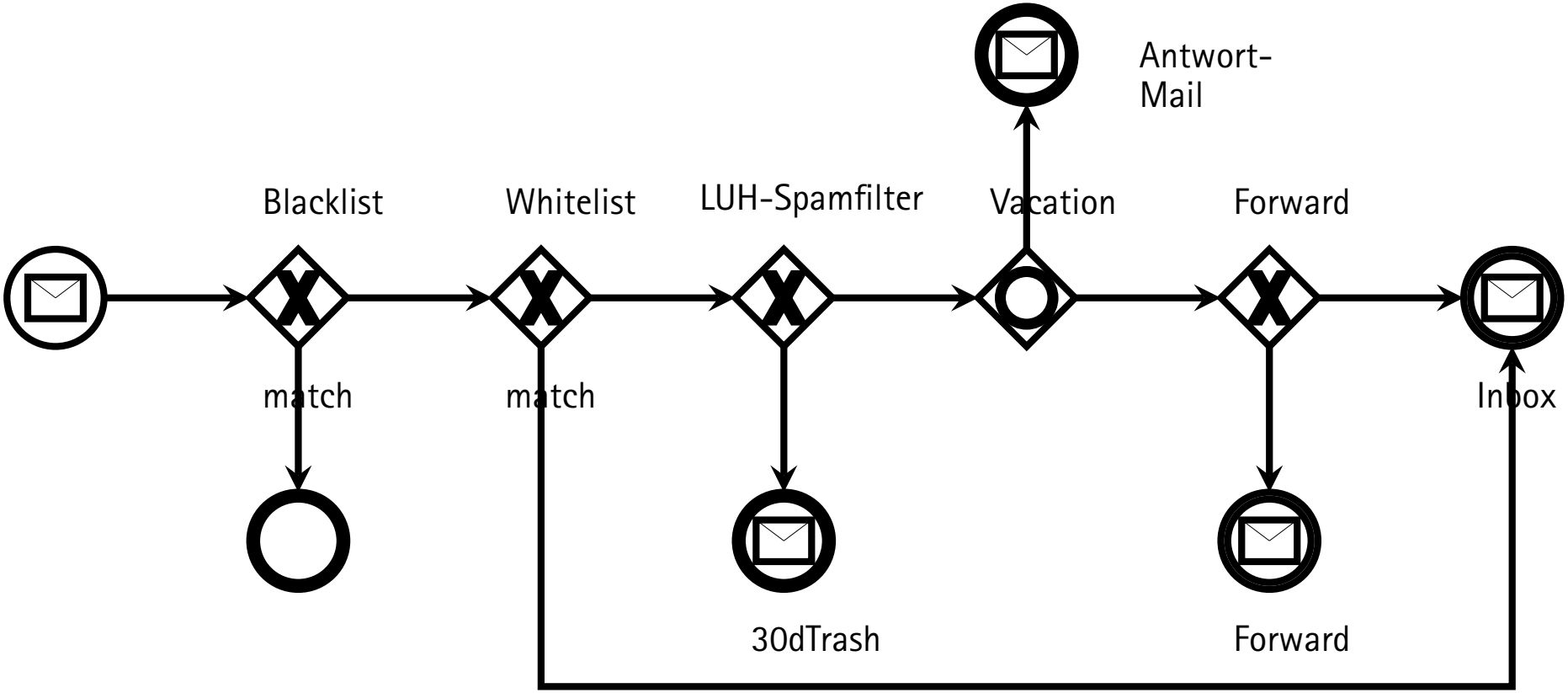
- eigene Spamabwehr-Versuche über White- & Blacklists
- Abwesenheitsmeldungen an alle, auch an Spammer
- ungültige, unwirksame Einträge

Empfehlungen nun detailiert auf unserer Webseite:

- Black- und Whiteliste nur in Ausnahmefällen nötig
- erst Spam-Abwehr, dann Abwesenheitsmeldung

Details vgl.
`http://www.rrzn.uni-hannover.de/email_filter_sieve.html`

Sortierung auf dem Mailserver



Mailheader – Filter-Policy

```
X-DFN-Virus-Scanned: Debian amavisd-new at mgw1-erl.srv.dfn.de
X-DFN-Spam-Flag: YES
X-DFN-Spam-Score: 9.351
X-DFN-Spam-Level: *********
X-DFN-Spam-Status: Yes, score=9.351 tagged_above=2 required=7
tests=[AWL=2.615, BAYES_50=0.8, HTML_IMAGE_ONLY_04=1.172, HTML_MESSAGE=0.001,
HTML_MIME_NO_HTML_TAG=0.01, HTML_SHORT_LINK_IMG_1=0.001, MIME_HTML_ONLY=1.2,
RCVD_IN_BRBL_LASTEXT=1.449, RDNS_NONE=0.793, SUBJECT_NEEDS_ENCODING=1.3,
T_REMOTE_IMAGE=0.01] autolearn=no
Received: from mfilter-112-1-3.mx.srv.dfn.de ([127.0.0.1]) by localhost
```

- RBL: Reject
- Virus: Prequeue Filtering → Reject
- Schwellenwerte für's Tagging:
  $\geq$2 Spam-Flag: NO, $\geq$7 Spam-Flag: YES
- Schwellenwerte für's Reject (Instanz 3): 8.5
- Optionales Sofort-Reject (langfristiges Ziel für alle Domänen)

Training für die Spamerkennung

- Spamassasin nutzt sogenannte lernfähige Bayes-Filter. Training erfolgt durch unsere Mailadmins.
- Senden (Weiterleiten oder Umleiten) Sie SPAM- und HAM-Mails inklusive kompletten Header an folgende Adressen:
- `spam@rrzn.uni-hannover.de`
- `ham@rrzn.uni-hannover.de`

Leibniz Universität Hannover

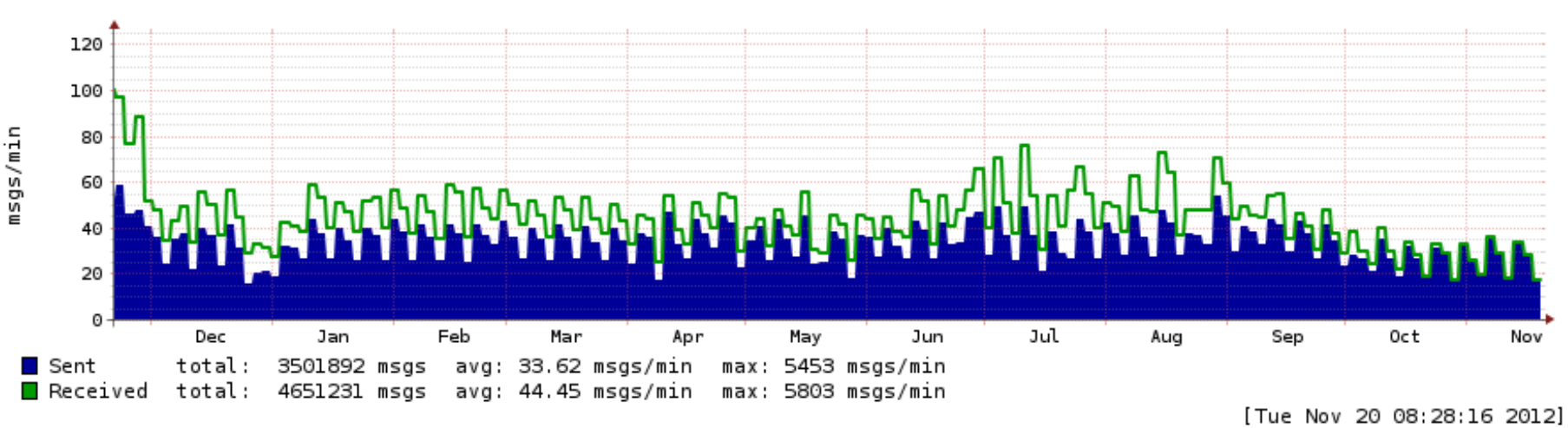
Eingehender durch Sophos erkannter SPAM seit Februar 2012:

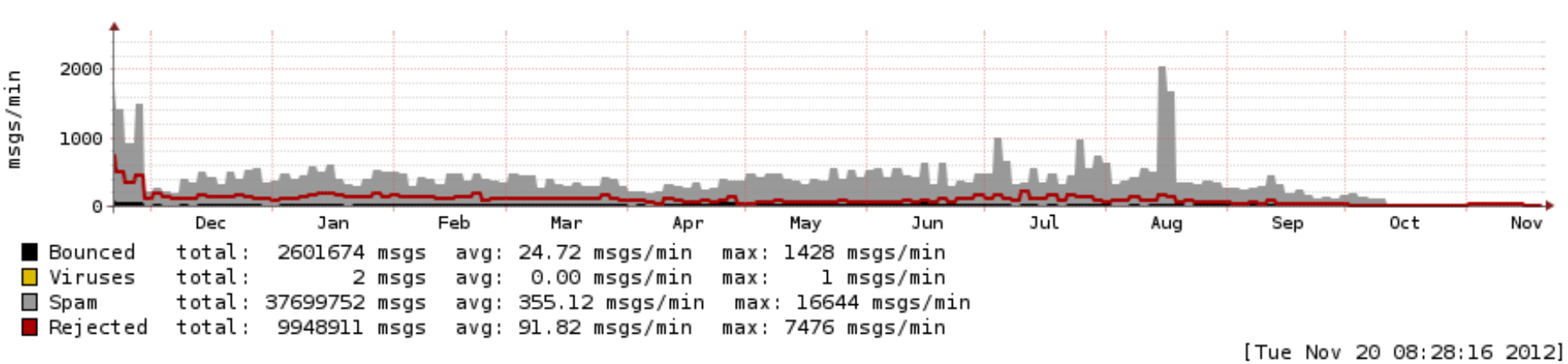
Februar	334875	Juni	21374097
März	1143258	Juli	29446106
April	1071289	August	30087505
Mai	666656	September	10629811

DFN SPAM-Abwehr der vergangenen Woche:

Reject	3365807
Spam-Flag: YES	11494
$\sum$	3377301

Zahlen


msgs/min
120
100
80
60
40
20
0
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
RRDTOOL / TOBI OETIKER
Sent total: 3501892 msgs avg: 33.62 msgs/min max: 5453 msgs/min
Received total: 4651231 msgs avg: 44.45 msgs/min max: 5803 msgs/min
[Tue Nov 20 08:28:16 2012]


msgs/min
2000
1000
0
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
RRDTOOL / TOBI OETIKER
Bounced total: 2601674 msgs avg: 24.72 msgs/min max: 1428 msgs/min
Viruses total: 2 msgs avg: 0.00 msgs/min max: 1 msgs/min
Spam total: 37699752 msgs avg: 355.12 msgs/min max: 16644 msgs/min
Rejected total: 9948911 msgs avg: 91.82 msgs/min max: 7476 msgs/min
[Tue Nov 20 08:28:16 2012]

Ausblick

Leibniz Universität Hannover

Mailsetup DFN → RZ

Softwarekomponenten DFN

DNS

User unknown – Postfix Recipient Address Verification

Sortierung auf dem Mailserver

Mailheader – Filter-Policy

Training für die Spamerkennung

Zahlen

Ausblick

Links

Leibniz Universität Hannover

Fragen & Wünsche

Anlässlich der Umstellung aufgeworfen:

- Bitte: Aufräumen von Alt-Accounts und Alt-Domains, im Hinblick aufs IdM auch Abgleich mit HIS-LSF
- Qualifiziertes User-Unknown von Instituts-Mailservern `550 5.1.1 <lskdjfksldjf@uni-hannover.de>: Recipient address rejected: User unknown in relay recipient table`
- POP3 sollte mittelfristig wegfallen
  - leave-on-server und zu häufiges Abfragen erzeugt Last
  - fetchmail, popcorn etc. können auch imap
- Macht Mail-Hosting ohne DNS-Hoheit zu große Probleme?
- Horde-Webmailer: Aktualisierung, evt. auch Ablösung

Absenden von Mails

Reglementierung bzgl. rausgehendem SMTP zur Verhinderung von Missbrauch für Spam

- unauthentifiziertes SMTP nur noch für wenige benannte Systeme (typischerweise Mailserver, bestimme Serveranwendungen)
- sonst unauthentifiziertes SMTP nur an LUH-interne Empfänger (typischerweise für Log-Mitteilungen, Cron-Jobs)
- Mailclients über authentifizierten Versand (Submission & TLS)
- direkte SMTP-Verbindungen in Internet unterbinden
- Rest loggen für Intrusion-Detection

. . . schrittweise Einführung, nur mit ausreichender Ankündigung

Links

Links

- DFN-Dienst:
  http://mailsupport.dfn.de
- SPAM-Abwehr am Rechenzentrumm:
  http://www.rrzn.uni-hannover.de/email_spamabwehr.html
- Wechsel des Anbieters am Rechenzentrum:
  http://www.rrzn.uni-hannover.de/email_pmx2dfn.html
- Filtern mit Sieve/Mailklienten:
  http://www.rrzn.uni-hannover.de/email_filter_sieve.html
  http://www.rrzn.uni-hannover.de/email_filter_clients.html