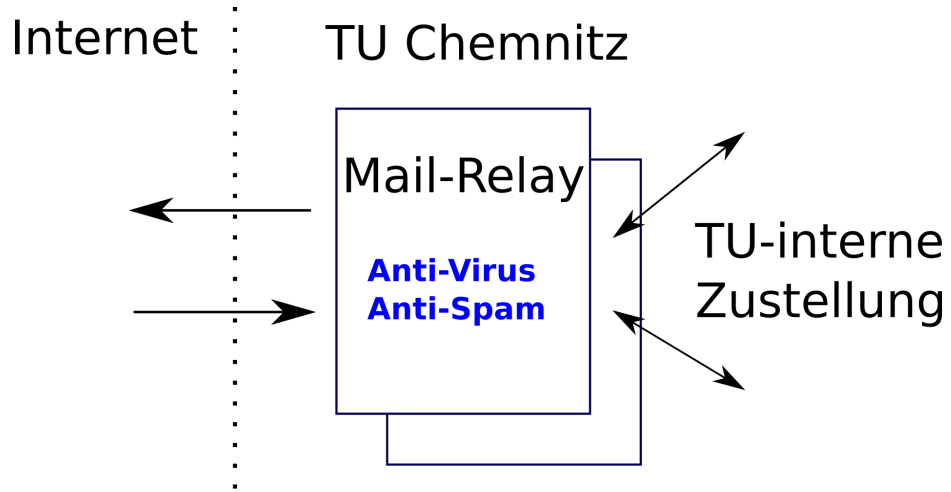
Erfahrungen mit dem DFN-Mailsupport an der TU Chemnitz

Frank Richter

Technische Universität Chemnitz – Universitätsrechenzentrum

77. DFN-Betriebstagung – Berlin, 18. Oktober 2022

Ausgangspunkt bis November 2021



- Anti-Virus: ClamAV
  - mit zusätzlichen Signaturen (`securiteinfo.com`)
- Anti-Spam:
  - Greylisting
  - DNSBL (`spamhaus.org` ...)
  - CYREN expurgate (Produkt zur Bewertung von E-Mails)
  - SpamAssassin
  - weiteres: HELO-Checks ..., eigene Listen

→ Ziemlich zufrieden

Insb. CYREN expurgate sorgte für:

- wenig Spam (außer Einzeiler . . .)
- kaum Phishing
- false positives sehr selten
- Aufwand überschaubar
- Greylisting zunehmend lästig (Adobe-Accounts)

Warum ändern?

- leider kein akzeptabler AVV mit CYREN abzuschließen
- externe Speicherung von Metadaten zu jeder E-Mail, Hash und URLs mit unklaren Speicherfristen und -orten

Ziele:

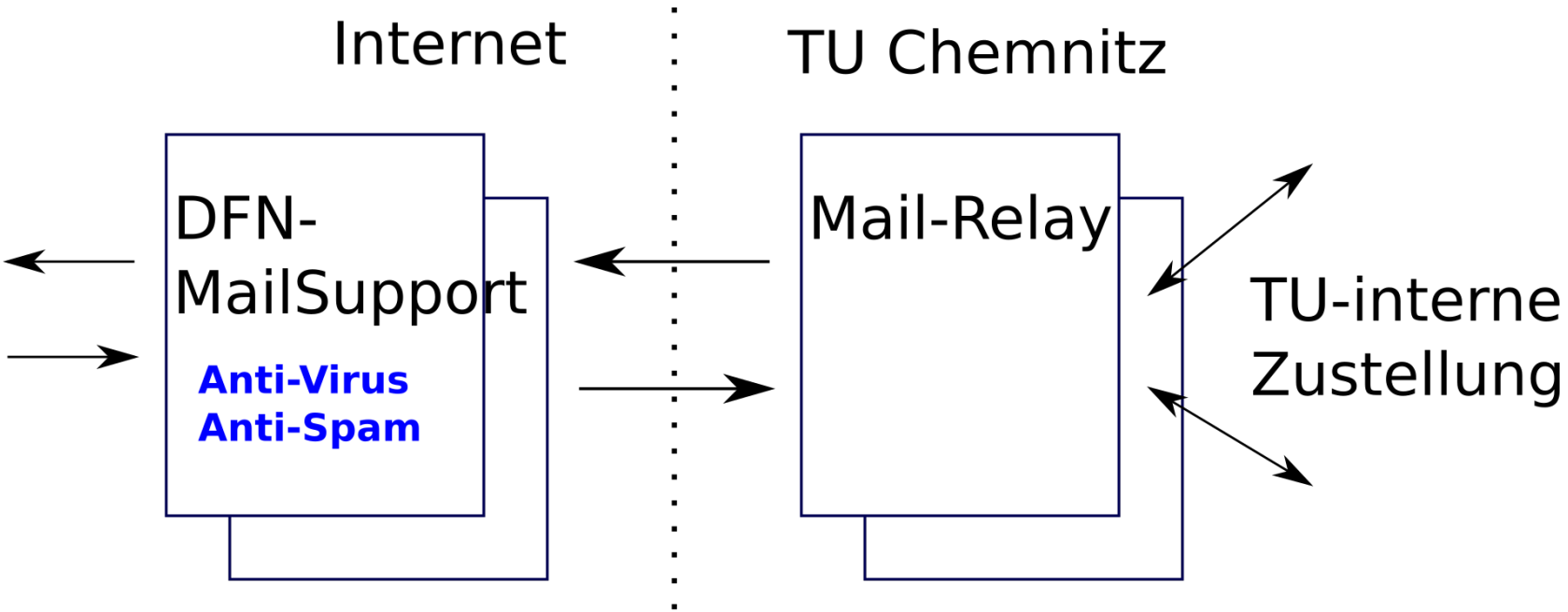
- möglichst gleichbleibender guter Schutz
- Datenschutz – AVV
- wenig(er) Supportaufwand
- Kosten sparen

→ Umstieg auf DFN-Mailsupport

- AVV für DFN-Mailsupport mit DFN abgeschlossen
- technische Vorbereitungen
  - Logging auf TUC-Server
  - neues Mail-Relay ohne Anti-Virus und Anti-Spam
  - Einstellungen im DFN-MailSupport-Portal
  - MX ändern

$\rightarrow$ ab November 2021 schrittweise (Sub-) Domains umgestellt, zunächst nur incoming

Neue Strukur mit DFN-Mailsupport



- kein Greylisting

Statistik

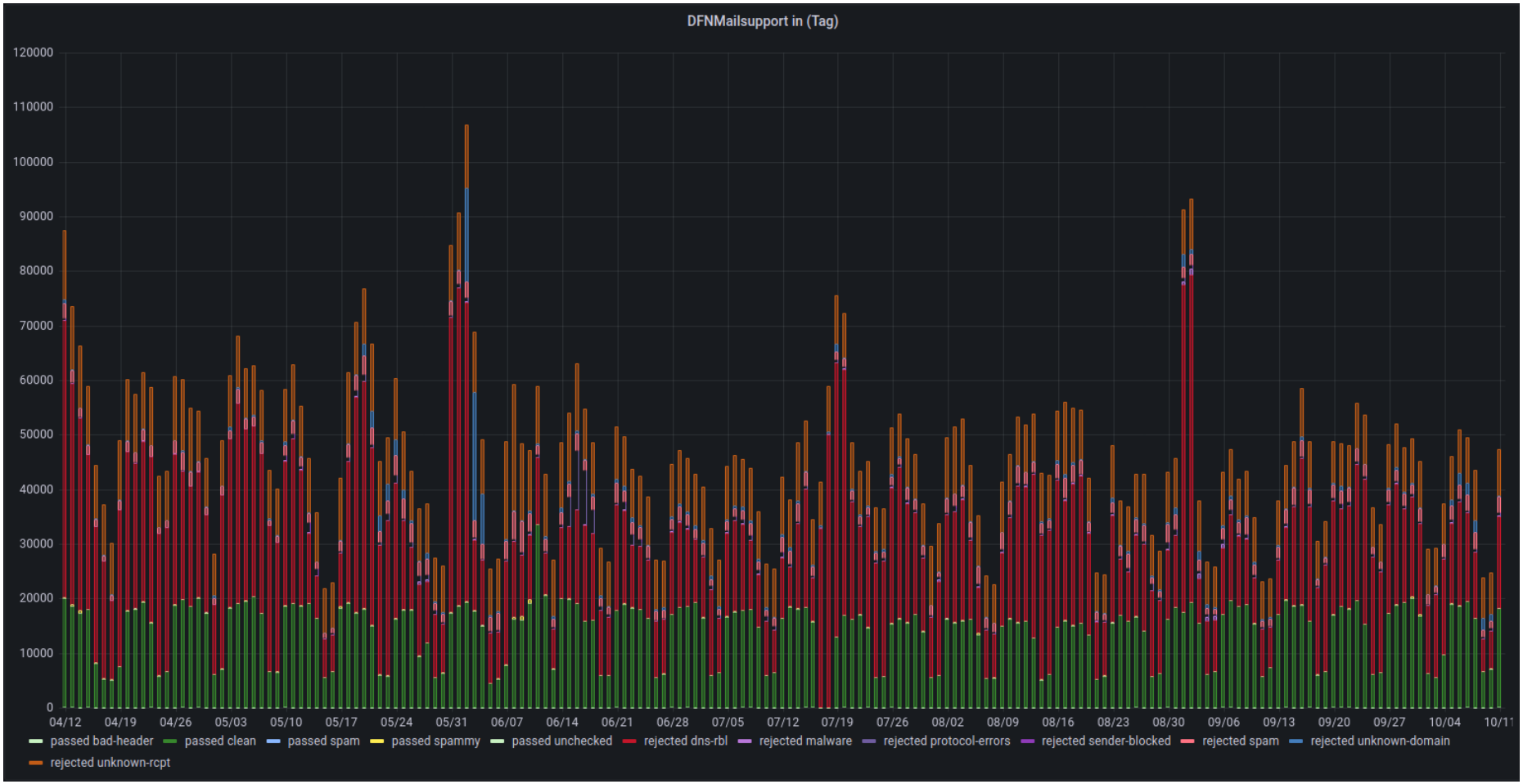


Abbildung: grün = angenommen, alles andere abgelehnt

Nutzer-Feedback

- „Spam kam bisher sehr selten, in den letzten 2 Wochen aber vermehrt …“
- Betroffen sind vor allem VIPs o. a. lang gültige E-Mail-Adressen.
- Alles dabei: Pharma, Porno, dubioses, leider viel Phishing
- Andere erhalten weiterhin wenige Spam-Mails.

→ Support-Aufwand bei uns ist leider gestiegen.

Test mit CYREN expurgate:

- ca 3% der via DFN-Mailsupport empfangenen E-Mails ist Spam
  → 400 bis 1000 Mails / Tag
- Gegenprobe fehlt

Dienstverfügbarkeit ist super!

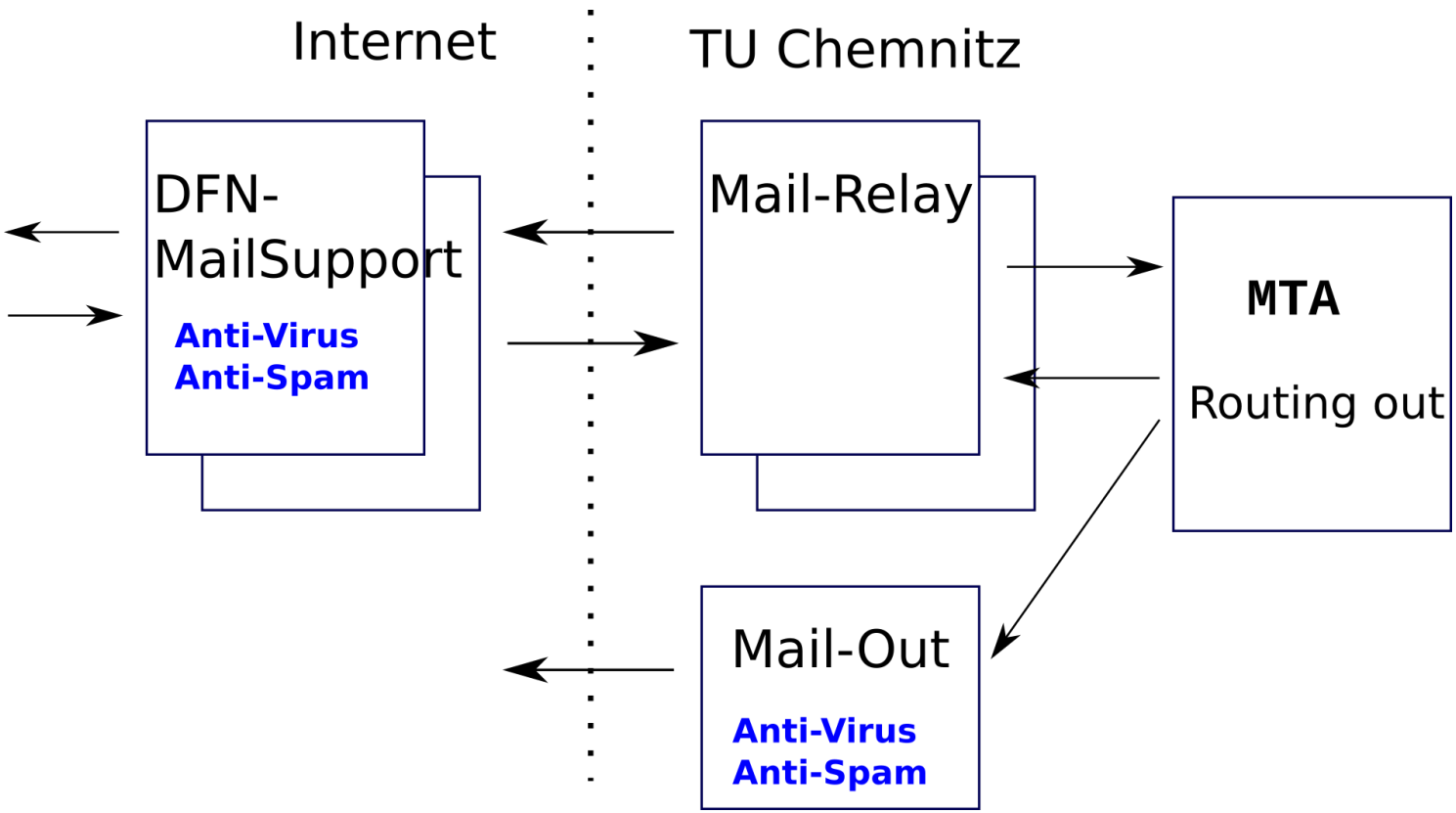
Zusammenarbeit mit den Kolleg/innen im DFN-Mailsupport ist gut:

- Beratung: Abwehr jetzt bei 7.0 Spam-Punkten (Spam-Limit): Problem bleibt leider
- 4 Wochen Greylisting aktiviert: keine (spürbare) Verringerung der Spamanzahl
- Anfang Juni: viele false positives – sehr unangenehm

Bayes-Filter trainieren:

- Täglich meldet das Mailteam zwischen 5 und 75 E-Mails als Spam beim DFN-Mailsupport
- . . . führt das zur Besserung?
- Problem: Ham melden – woher nehmen?

- schrittweise für Absender-Domains umgestellt
- Ratelimits zwingend: Vielsender melden
- einige Absender, wie Lernplattform, Studentenwerk . . . versenden wir direkt ohne DFN-Mailsupport



Fazit

Ziele erreicht?

- möglichst gleichbleibender guter Schutz ×
- Datenschutz – AVV ✓
- wenig(er) Supportaufwand ×
- Kosten sparen ✓ … ×

Wünsche

- Besserer Schutz insb. vor Phishing-Mails und immer wiederkehrender Spam

  Paretoprinzip (80/20): Die letzten Prozente in der Abwehr von schädlicher und unerwünschter E-Mail verursachen hohen Aufwand.

- höheres Schutzniveau auch kostenpflichtig

- Ankündigung von technischen Änderungen, z. B. über Mailing-Liste
- API über alle Parameter, die über die GUI eingestellt werden können