

Spam-Filterung

Sonderveranstaltung

**Dr. Gabriele Dobler, Dr. Reiner Fischer,
Ulrich Nehls, Gunther Heintzen**

12.Dezember 2003



- Entwicklung des Mail-Aufkommens
- Ziele des RRZE
- Spam-Bewertung / Spam Filter
- Grenzen der zentralen Spam-Analyse
- X-Spam-Header für Filter
- Spam-Analyse-Protokoll
- Spam filtern am E-Mail Client
 - Mozilla/Netscape
 - Pegasus
 - Outlook
- Allgemeine Hinweise
- Weitere Informationen

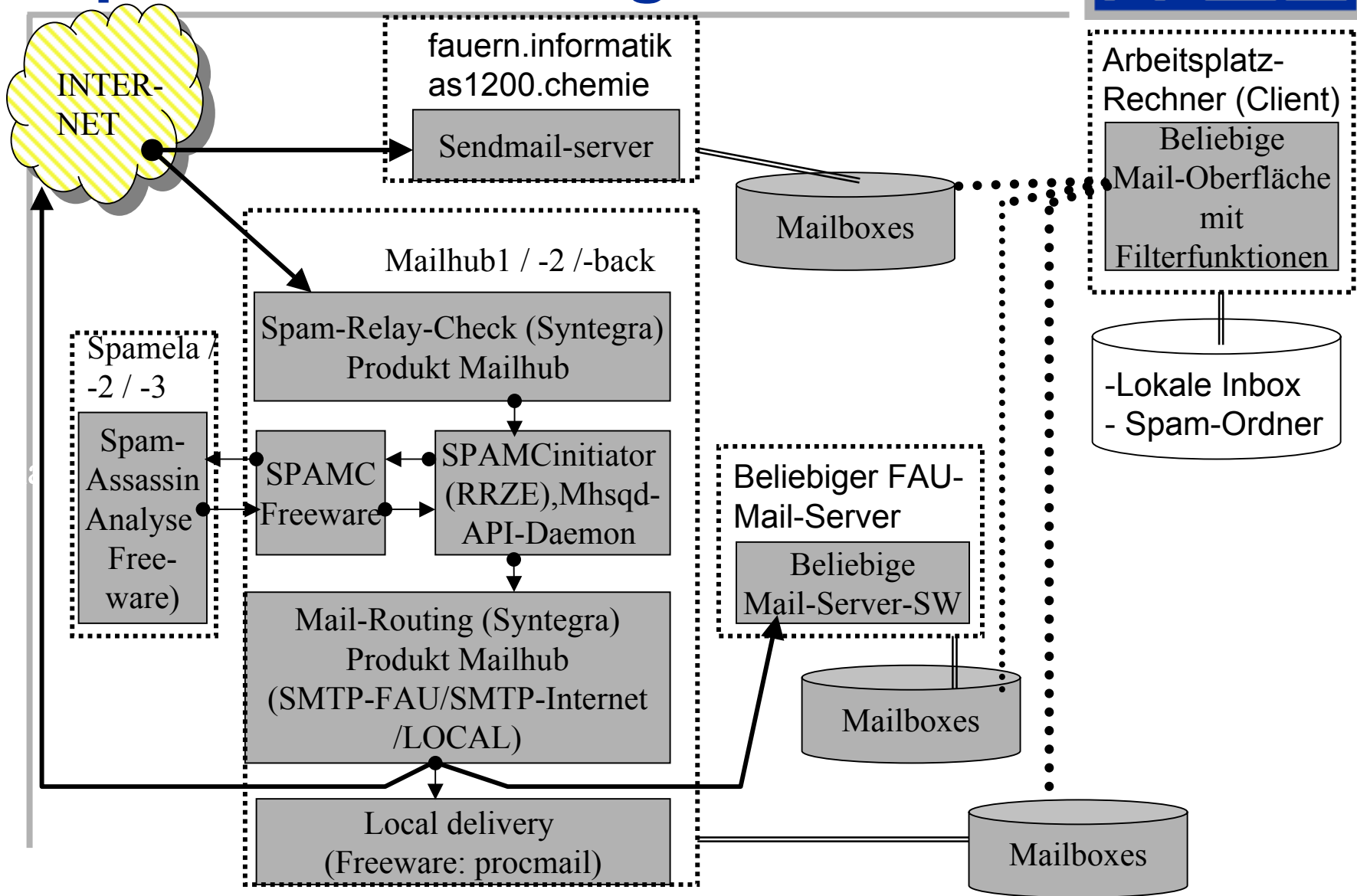


- Am FAU-Mail-Relay mehr als 200.000 Mails pro Tag
- Mehr als 60 % davon sind als Spam einzustufen
- Was ist Spam? Diese Frage entscheidet jeder Empfänger selbst
- Die Spam-Einschätzungen vieler Empfänger sind ähnlich



- Entlastung der Empfänger
 - Einführung einer Spam-Analyse am Mail-Relay mit zentral gepflegten Bewertungskriterien
 - Hilfestellung beim Einrichten von Filtern
- Stabilität und Zuverlässigkeit am Mail-Relay
 - Vermeiden von Überlast aufgrund von Spam-Attacken
 - Zeitnahe Zustellung / Weiterleitung „erwünschter“ E-Mails
 - Kein Risiko bzgl. Verlust erwünschter E-Mails
- Wahrung von Recht und Gesetz
 - Veränderungen des Mail-Inhaltes nur im Auftrag des Empfängers
 - Löschen darf nur der Empfänger
 - „Stempeln“ von E-Mails verändert den Inhalt nicht !

Spam: Bewertung / Filter





- Keine Bewertung, wenn
 - Dauer der Analyse Zeitlimit überschreitet;
 - Größe der Mail Maximalgröße überschreitet;
 - E-Mail am zentralen FAU-Mail-Relay vorbei ins FAU-Kommunikationsnetz gelangt (fauern, as1200)
- Qualität der Bewertung
 - Regelbasierte Analyse von Header und Body ist nie vollständig (Release-Wechsel)
 - Blacklists basieren auf weltweiten Statistiken über Hosts, die als „Spam-Schleuder“ auffallen.
 - Spam-Datenbanken speichern Charakteristik von Spam-Mails in Abhängigkeit von der Häufigkeit
 - Bayes Filter ermitteln anhand einer lexikalischen Analyse einen Wahrscheinlichkeitswert



Zusätzliche Informationen von SpamAssassin im Nachrichtenkopf (Header)

- **X-Spam-RRZE-Info:**
Diese Mail wurde einer automatischen Spam-Analyse unterzogen, siehe:
<http://www.rrze.uni-erlangen.de/SPAM-Analyse/>
- **X-Spam-Checker-Version:**
SpamAssassin 2.60-rrze_02(1.174.2.19-2003-05-19-exp)on
spamela2.rrze.uni-erlangen.de
- **X-Spam-Flag:** YES
- **X-Spam-Level:** *****



- **X-Spam-Status:**

Yes, hits=10.2 required=5.0

tests=DATE_IN_FUTURE_03_06, DCC_CHECK,
FORGED_MUA_OUTLOOK, HTTP_EXCESSIVE_ESCAPES,
MISSING_MIMEOLE, SEMIFORGED_HOTMAIL_RCVD
version=2.60-rrze_02

- **X-Spam-Report:**

---- Start SpamAssassin results

10.20 points, 5 required;

* 0.6 -- URI: Completely unnecessary %-escapes inside a URL

* 3.0 -- Listed in DCC, see <http://rhyolite.com/anti-spam/dcc/>

* 1.7 -- hotmail.com 'From' address, but no 'Received:',

* 0.9 -- Date: is 3 to 6 hours after Received: date

* 0.5 -- Message has X-MSMail-Priority, but no X-MimeOLE

* 3.5 -- Forged mail pretending to be from MS Outlook

---- End of SpamAssassin results

Filtern am E-Mail Client



- Mozilla/Netscape (hier: Mozilla 1.2.1)
- Pegasus (hier: Pegasus 3.XX)
- Outlook (hier: Outlook 2003)

Hier folgt eine Online-Vorführung, deren Snapshots unter <http://www.rrze.uni-erlangen.de/Spam-Analyse> zu finden sind.

Outlook wird vom RRZE nicht empfohlen!

Von der Benutzung von Outlook Express raten wir dringend ab, es wird nicht unterstützt!



Tips zum Verfassen von E-Mails:

- Immer einen Betreff angeben
- Copy & Paste vermeiden
- Automatischer Zeilenumbruch kann zu sehr langen Zeilen führen
- Text Mails verfassen oder nur wenig HTML einbinden



Dieser Vortrag

<http://www.rrze.uni-erlangen.de/netze/email/Vortraege/SpamFiltern.pdf>

Anti-Spam Dokumentation des RRZE

<http://www.rrze.uni-erlangen.de/SPAM-Analyse>

SpamAssassin

<http://www.spamassassin.org>

Razor

<http://razor.sourceforge.net>

Distributed Checksum Clearinghouse

<http://rhyolite.com/anti-spam/dcc/>