SPONTS

Kurt Huwig
Vorstand
iKu Systemhaus AG

Was ist SPONTS

- SPONTS ist ein
  - Linux-basierter
  - modularer
  - SMTP-Proxy

Linux-basiert

- gehärtetes Linux auf Debian/Woody-Basis
- hohe Stabilität
- hohe Sicherheit
- kleiner Speicherbedarf (9 MB Festplatte)

Modular

- Module
  - UCE (Spam-Schutz)
  - Replay (Online-Backup)
  - UMS (Not-Zugriff)
  - Journal (Protokollierung)
  - Report (Statistiken)

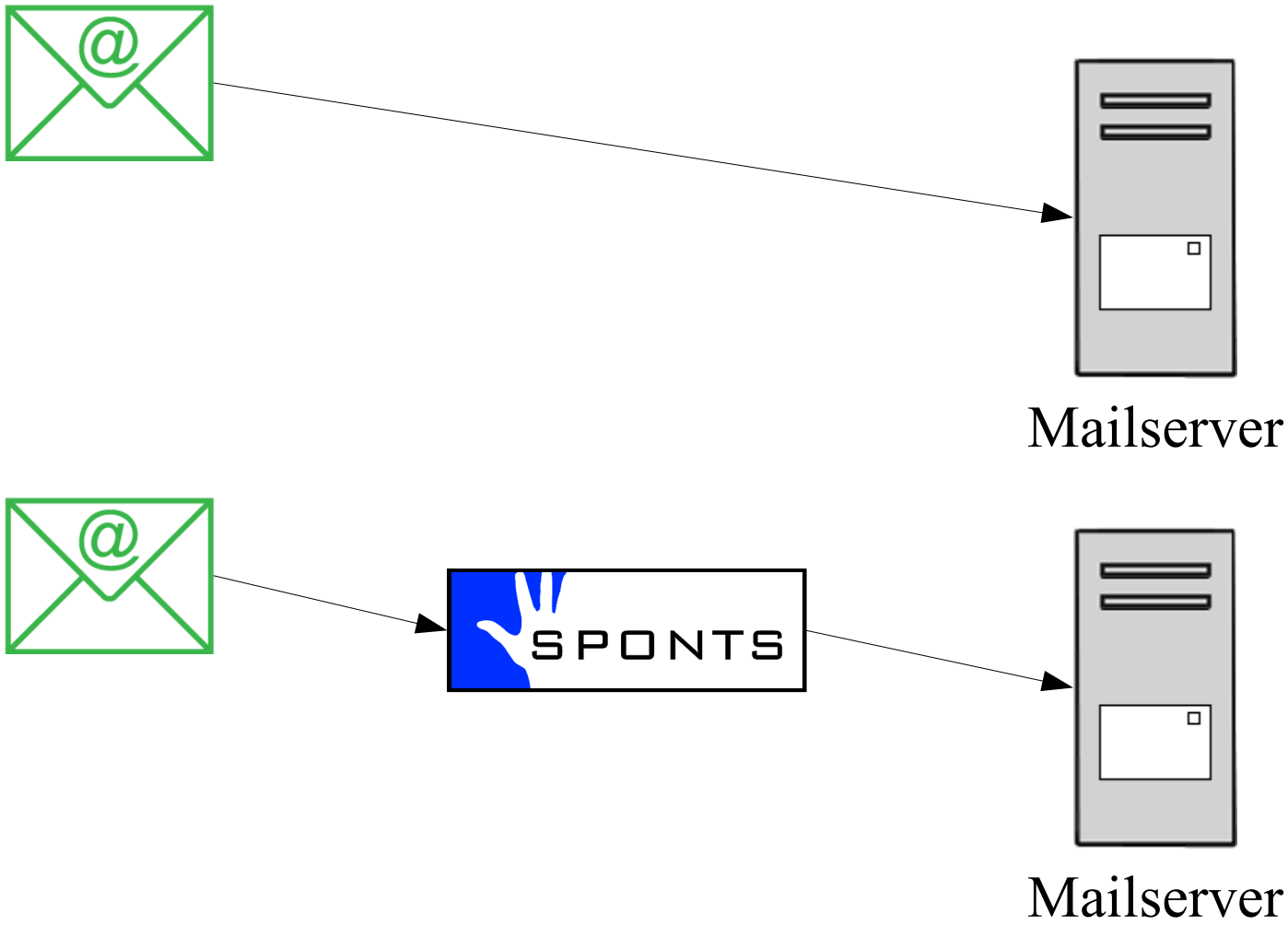
auch erhältlich als Appliance

- Software mit Hardware
- fertig installiert
- passiv gekühlte CPU
- Flash-Chip an Stelle einer Festplatte
- hohe Ausfallsicherheit

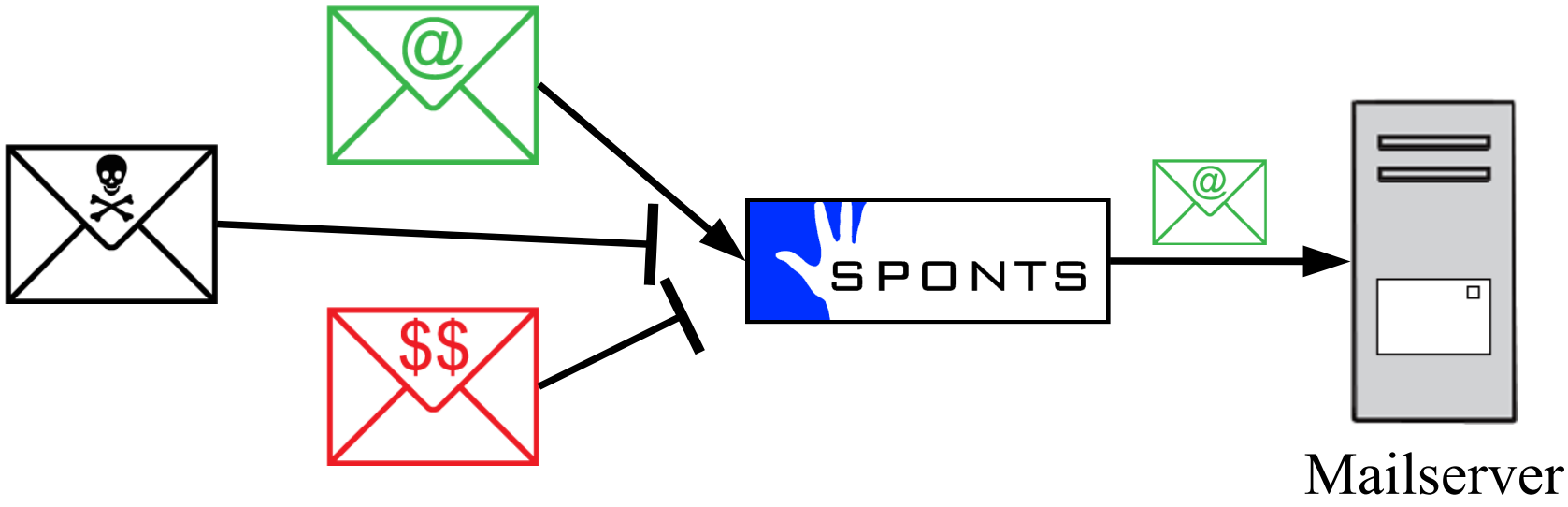
Datenhaltung in SQL

- leichter Zugriff
- leichte Auswertungen
- leichte Integration in eigene Anwendungen
- leicht zu sichern
- hoch performant

SMTP-Proxy

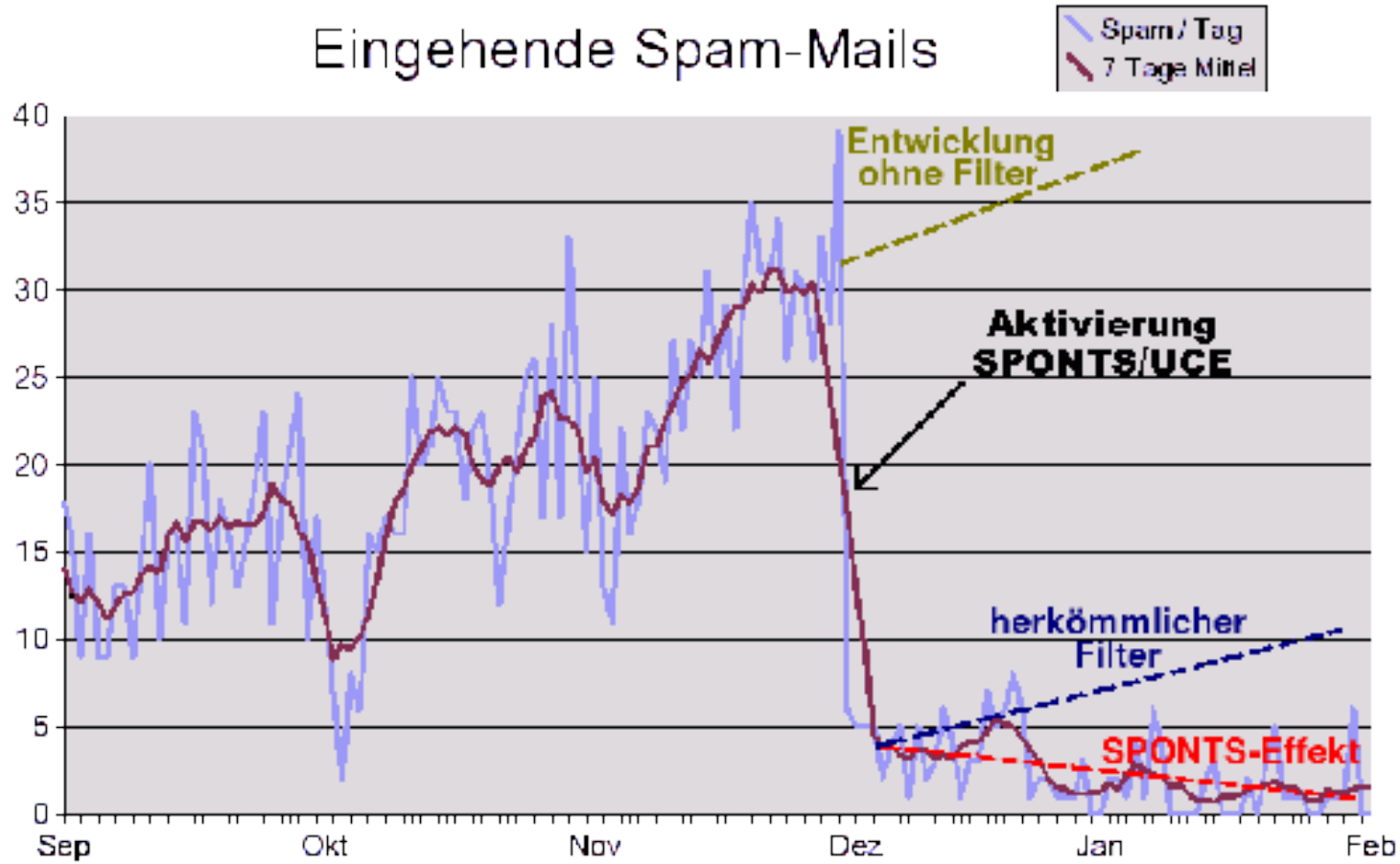


Böses muss draußen bleiben



Dauerhafte Spam-Reduzierung

- "mich gibt es nicht"



Funktioniert das wirklich?

- Woher bekommen Spammer die Adresse?
  - gekaufte Adresslisten
  - Mail-Adressen von Webseiten, Mailing-Listen

gekaufte Listen

- “25 Millionen Adressen für 50$!”
- werden von Spam-Neulingen verwendet
- Neulinge machen Fehler, die eine Erkennung leicht machen

Adressen von Webseiten

- Spam von Profis wird schlecht erkannt
- Profi-Spammer verwenden eigene Spider um eigene Listen aufzubauen
- Profi-Spammer achten darauf, ob das Postfach existiert
  - der durchschnittliche Amerikaner wechselt alle 2 Jahre den Job
  - nicht existierende Adressen werden aussortiert

Fazit: es funktioniert

- Spam-Neulinge reagieren nicht drauf, werden aber leicht erkannt
- Spam-Profis sind schwer zu erkennen, reagieren aber darauf

weitere Gegenmaßnahmen

- Wegwerf-Adressen
  - it-profits.20.kurt@huwig.de
  - erlaubt 20 Mails
  - sperrt sich automatisch
  - für Spammer wertlos
- Adress-Verschleierung auf Webseiten
  - Spider erkennen die Adresse nicht mehr
  - kurt<img src=”gibt es nicht” alt=”@”>huwig.de

aktive Gegenmaßnahmen

- Spam-Traps
  - Lock-Adressen, die nur von Spammern gefunden werden
  - kurt@huwig.de
- ankommende Mail ist immer Spam
- Mail wird generell nicht weitergeleitet

aktive Gegenmaßnahmen

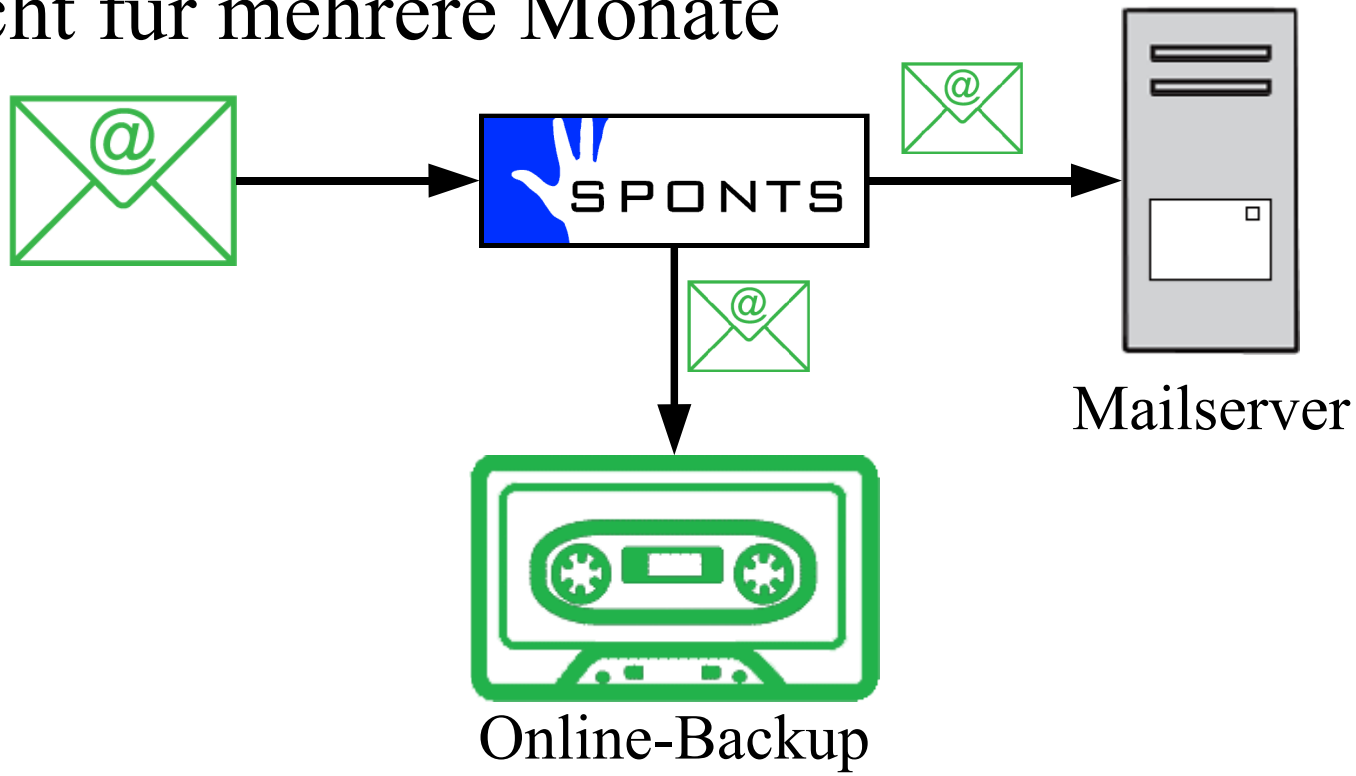
- Teergruben
  - bremsen Spammer aus
- Verbindungen zurück
  - “Spam zurückschicken”
- Webseiten in der Mail aufrufen
  - verursacht Traffic
  - Traffic für Spammer ist teuer

Ergebnis der Gegenmaßnahmen

- Spammer brauchen mehr Zeit
- Spammer brauchen mehr Traffic
- Spam wird besser aussortiert
- weniger Verkäufe
- **Spam wird teurer für den Spammer**

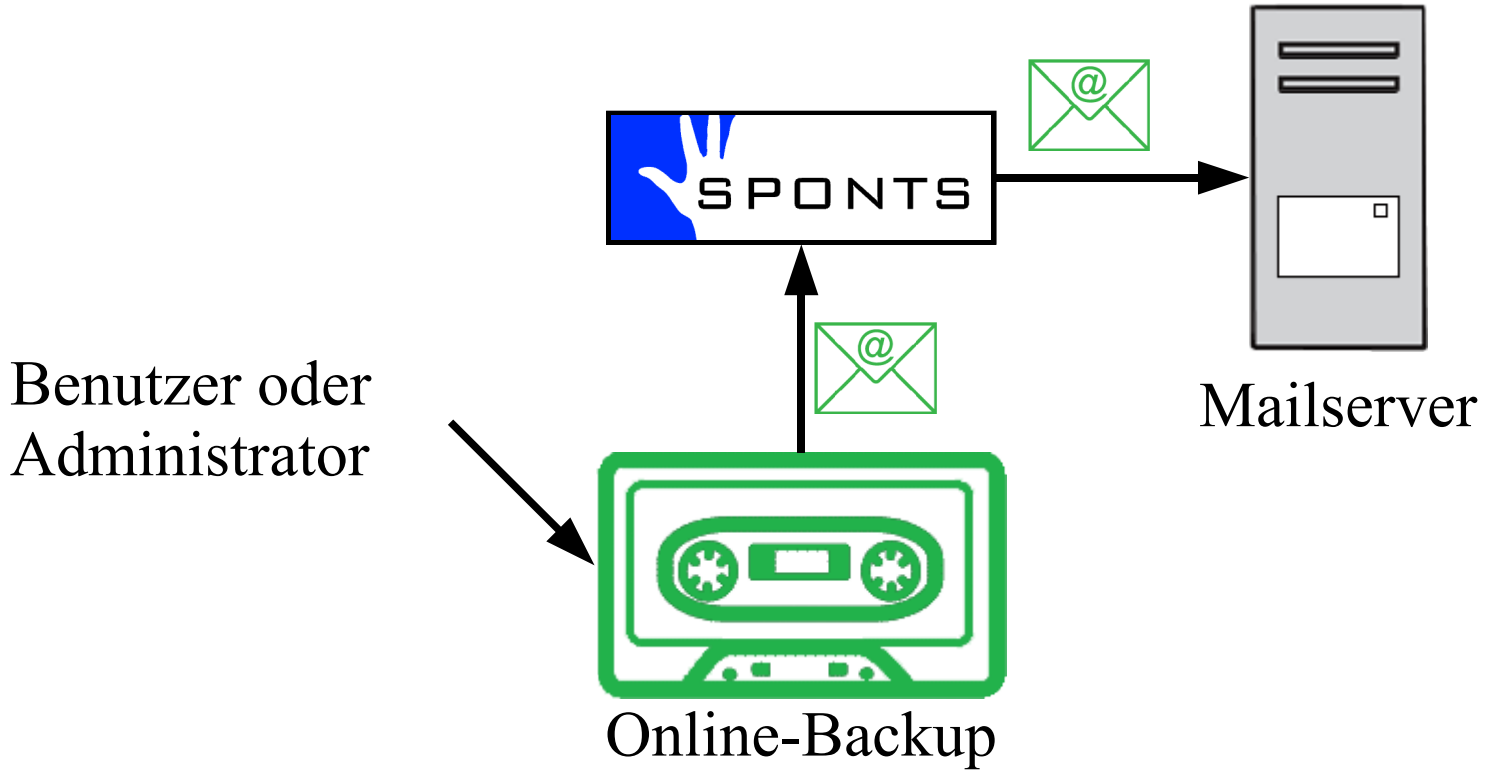
Online Backup

- Sicherheitskopie jeder Mail wird auf die Festplatte gesichert
- reicht für mehrere Monate



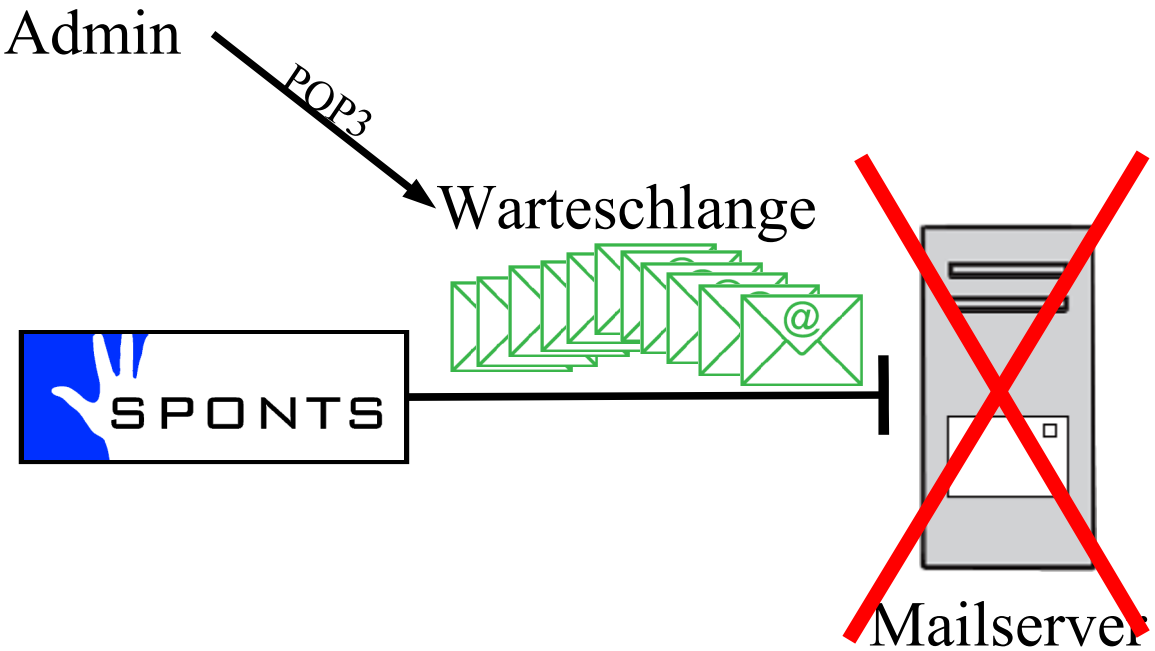
Replay aus dem Backup

- mit wenigen Klicks in Sekundenschnelle
- durch Benutzer oder Administrator



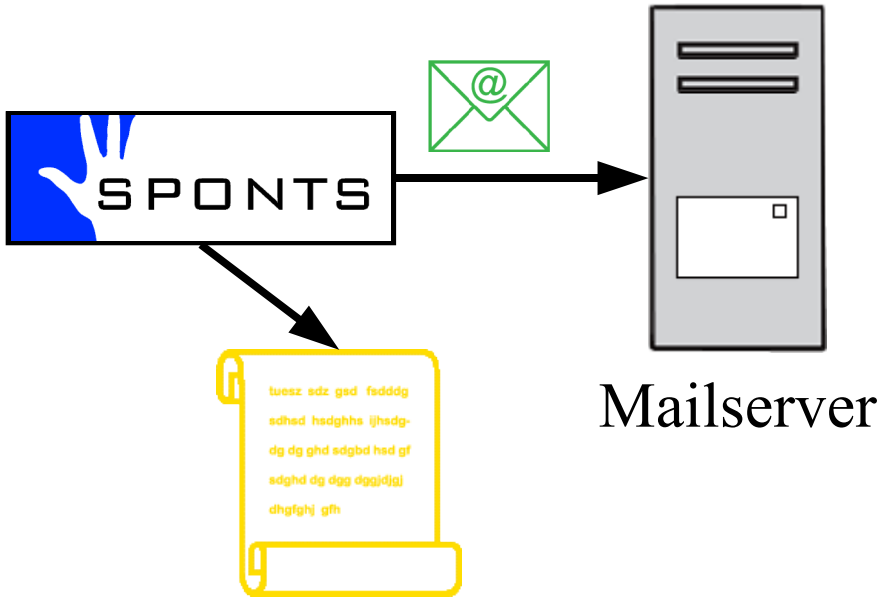
Notzugriff

- bei Ausfall des Mailservers
- Zugriff auf alle neuen Mails
- POP3 mit jedem Mailprogramm



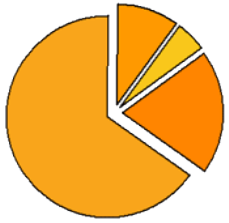
Umfangreiche Protokollierung

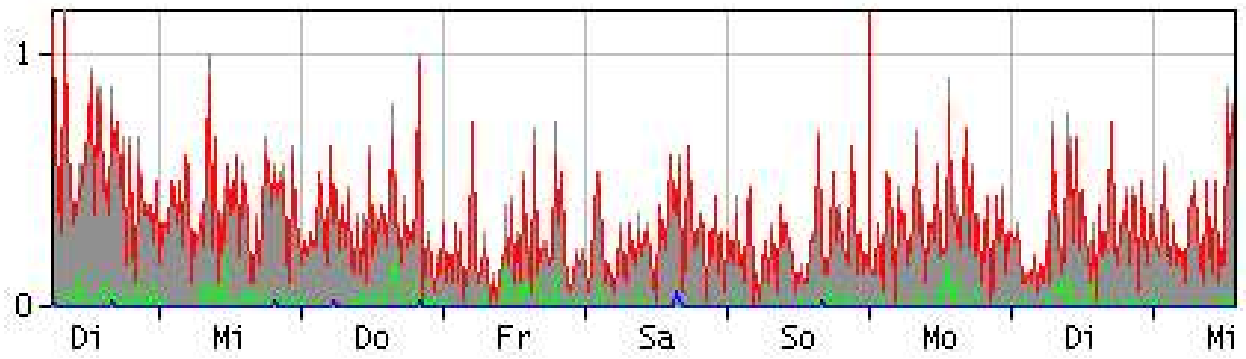
- Absender, Empfänger
- Datum, Uhrzeit, IP-Adresse
- Betreff
- Anhänge mit Dateiname und -größe



Umfangreiche Statistiken

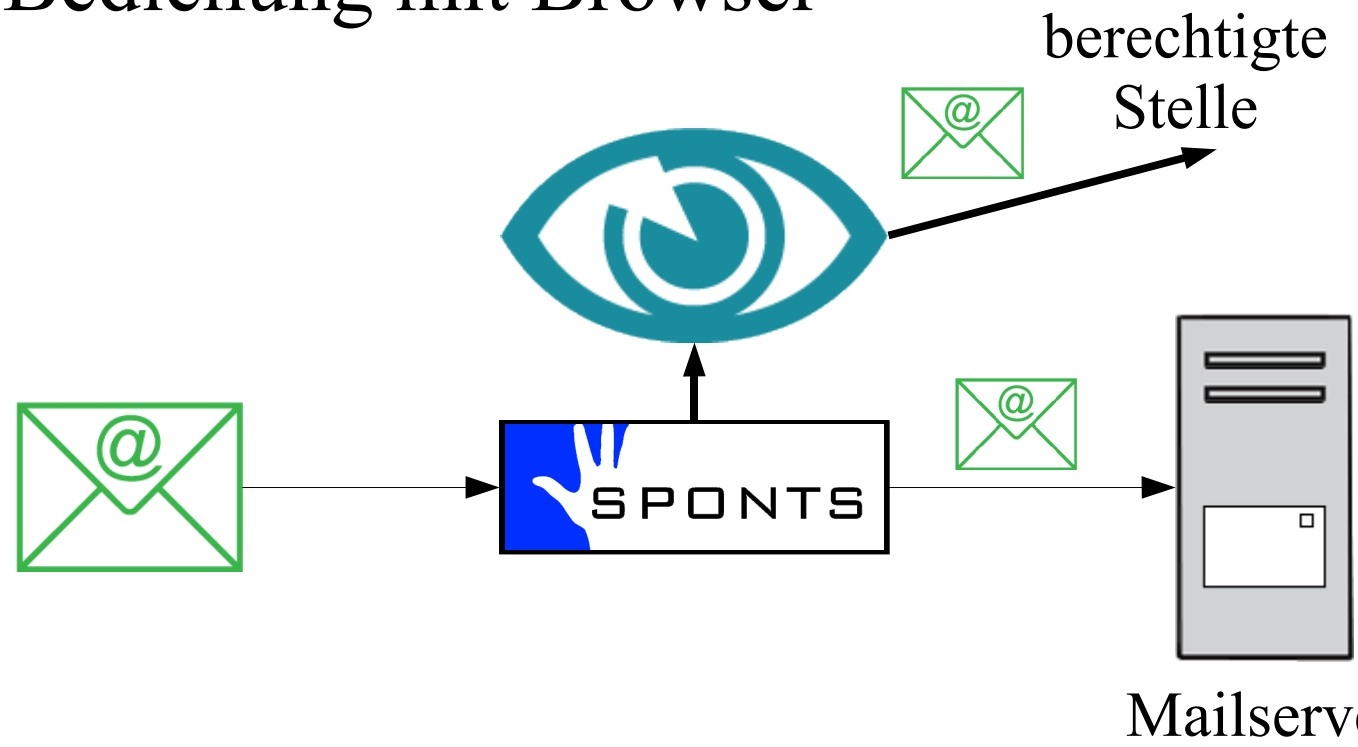
- Spam-, Viren-, Normal-Raten
- Auslastung ein- und ausgehend
- Last Virenscanner
- Top-Spammer





RegTP-zertifizierte TKÜV-Lösung

- Überwachung aller Protokolle
  - SMTP, POP3, IMAP - auch per SSL und TLS
- einfache Bedienung mit Browser



Demonstration
Fragen? Antworten!