Rezentralisierung von E-Mail-Services

Michael Storz

Team-Leiter E-Mail

Leibniz-Rechenzentrum

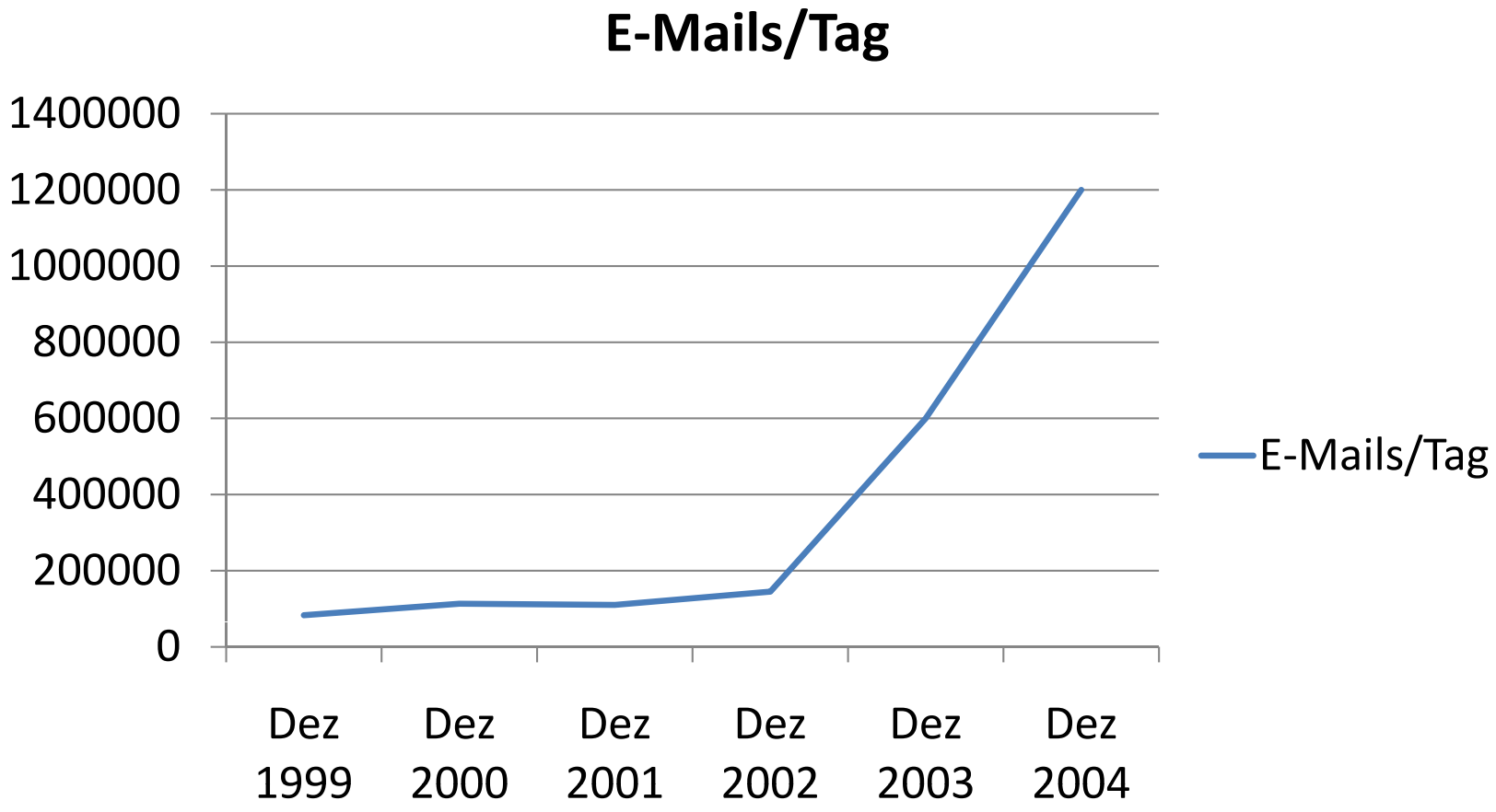
Ausgangssituation (1)

- bis 1994 virtuelle Maildomains (X.400) am LRZ für Mitarbeiter der TUM
- seit 1995 virtuelle Maildomains (SMTP) (Mailserver mailin, 2004: 60 Domains)
- seit 1997 zentraler Mailserver für Studenten der TUM
- Okt 2003 Studentenserver abgelöst durch myTUM-Mailserver für Studenten (mytum.de) und Mitarbeiter (tum.de/mytum.de) mit LDAP
- 2004 ca. 100 lokale Mailserver der TUM

➔ 3 verschiedene Arten an Mailservern für TUM

Ausgangssituation (2)

dramatischer Anstieg an Spam-/Virenmails



Ziele (1)

- Genau eine Mailbox pro Mitarbeiter
- Entlastung der Admins an den Lehrstühlen
- Zusammenlegung der für die TUM am LRZ betriebenen Mailsysteme
- Erhöhung der Qualität des Mailservices
- Integration in TUM-weites Identity-Framework

➔ Rezentralisierung der Mailservices auf hochverfügbares und skalierendes Mailsystem am LRZ

Ziele (2)

- Abwehr von Spam und Viren
  - Filterung aller E-Mails an zentraler Stelle auf Viren.
  - Soweit wie möglich Abweisung von Spammails bevor sie von den Mailrelays des LRZ angenommen werden.
  - Markierung aller trotzdem angenommenen Spammails, um sie lokal in einen Spam-Folder verschieben zu können.

Spam- und Viren-Filterung

- 27.01.2004: Ausbruch MyDOOM ➔ 90.000 Virenmails/Tag
- Frühjahr 2004: Migration Mailrelays auf neue Hard- und Software, Umstieg von X.500 auf LDAP, Filterung von Viren über reguläre Ausdrücke auf Header/Body
- Juni 2004: Einsatz von Sophos zur Virenfilterung auf den Mailrelays
- Oktober 2004: Bewertung aller E-Mails mit Hilfe von SpamAssassin, Markierung aller Spammails
- myTUM-Mailserver: automatisches Verschieben von Spammails in Spam-Folder sofern von Benutzer gewünscht
- Beginn Implementation von Greylisting

Greylisting

- Greylisting bewertet die korrekte Ausführung eines Retrys nach einem temporären Fehler.
- Spamsoftware war/ist nicht in der Lage einen korrekten Retry durchzuführen ➔ Spammails werden nicht angenommen
- Check des Triples sendende IP-Adresse, Absender- und Empfangsadresse
- Feb 2005: Greylisting geht für alle E-Mails in Produktion

Greylisting Highlights

- strenges Greylisting, kein automatisches whitelisting für /24-IP-Netze
- Erweiterung von Sqlgrey um 2 weitere Auto-White-Lists (AWL)
- Erweiterung um zusätzliche Verfahren zur schnelleren Auffüllung der AWLs
- umfangreiche statische Whitelist für große ISPs (1.371 Mailserver-Netze)

Greylisting Erfolg

- Ablehnung von Spammails > 90 %
- Anteil verzögerter E-Mails
  - Beginn mit 11 % statt 100 % durch Vorbefüllung der AWLs
  - nach 4 Std. < 8 %
  - nach 2 Wochen < 5 %
  - später ca. 1,5 % (ohne angenommene Spammails)
- False-Positive-Rate: ca. 1 pro Woche

Greylisting Probleme

- März 2006: Botnet wiederholt 4 Mal im 5-Minuten-Takt ➔ Delay-Zeit von 14 auf 29 min
- Nov 2006 – März 2007: Replay-Attacke des Botnets SpamThru mit Pennystock-Spammails
- Mitte 2007: Brute-Force-Angriffe eines Botnets
  ➔ bei 1.000.000 E-Mails/Stunde Grenze des Greylistings erreicht
  ➔ Ursache: Bottleneck beim Pfad zwischen Hauptspeicher und CPU des MySQL-Servers

Postrelays

- neue Mailrelays auf Basis von Postfix
- vorgeschaltet vor die alten Mailrelays
- Sep 2007: Domains mytum.de und tum.de als erste Domains über neue Postrelays
- es folgen:
  - ei.tum.de/e-technik.tu-muenchen.de (Exchange)
  - ph.tum.de (Physik-Server)

Postrelay Checks

- Checks
  - 80 %: Ablehnung von dynamisch vergebenen IP-Adressen (DNSBL pbl.spamhaus.org)
  - 14 %: Forward-Confirmed reverse DNS (FCrDNS)
  - 5 %: Empfangs-Adresse (Vermeidung von Backscatter)
  - 1 %: Greylisting
- Whitelist für FCrDNS aus Greylisting-Database erstellt (4.500 Einträge)
- False Positive: 1/Woche bei FCrDNS, 0 bei PBL
- Okt 2008: 30 Mio Rejects/Tag, Peak 55.000/min

Pilotkunde Physik

- Juli 2005, nach längerer Vorbereitung Migration des Physikmailservers ans LRZ
- Einsatz des neuen Produktes IntraStore mit Webmail und webbasierter Administration
- dedizierte LDAP-Instanz mit Master-Master-Replikation
- Mailserver hochverfügbar ausgelegt
- Verwaltung der Benutzerdaten durch Physik-Admins über direkten LDAP-Zugriff

Syntegra

- Übernahme von Syntegra durch BT in 2004
- Probleme bei der Fehlerbehebung
- Kein De-Installation eines Patches möglich
- langsame bzw. keine Weiterentwicklung des Produktes IntraStore
- ISP-Modell nicht für TUM geeignet, benötigt wird Kooperation von virtuellen Maildomains
- kein funktionierendes Kalendermodul

➔ Ende 2006 Notbremse, Abkehr von Syntegra

Gruppenkalender

- nach Beginn des IntegraTUM-Projekts vermehrt Wunsch nach Gruppenkalender

  ➔ erste Lehrstühle migrieren vom LRZ weg und bauen lokale Groupware-Server auf
- Frühjahr 2006 Beginn Untersuchung von „stand alone“ Kalenderservern zur Integration in IntraStore ➔ Test von eGroupware
- nach Wegfall von IntraStore, Wunsch nach integriertem Groupware-Service

Groupware-Service

- Evaluation von Lotus Domino, Open Xchange und Microsoft Exchange
- Testinstallationen von Open Xchange und Microsoft Exchange
- Erstellung von Deploymentszenarien und Preiskalkulationen
- Vorstellung der beiden Alternativen in verschiedenen Gremien der TUM

➔ Juli 2007 Entscheidung der TUM für MS Exchange

Exchange (1)

- Aufbau eines mandantenfähigen Servers
- Mandanten sind TUM, LMU, LRZ und BAdW
- Mandanten sind von einander separiert, Kooperation kann aber durch Exchange-Admin eingerichtet werden
- Anbindung an Active Directory, das durch das Meta-Directory provisioniert wird
- Pilotkunde ist Fakultät für Elektrotechnik und Informationstechnik (Domain ei.tum.de)

Exchange (2)

- Produktionsbeginn verzögert sich durch die Einführung von TUMonline, da
  - die Provisionierung des Meta-Directorys umgestellt werden muss
  - die self services in TUMonline realisiert werden
  - es noch keine Admin-Services gibt
- Aufnahme weiterer Kunden aus anderen Fakultäten mit eigener Domain
- manuelle Administration der User/Ressourcen

Alumni

- Alumni der TUM können ihre E-Mail-Adresse lebenslang behalten
- keine Mailbox, nur Weiterleitung
- Verwaltung von Weiterleitung auf Exchange schwierig, da externe Adressen nur einmal vorkommen dürfen
- Problem mit Lizenzkosten

➔ Forwarder vor Exchange übernimmt Weiterleitungen der Alumni

Forwarder

- Wunsch:
  - freie Wahl, ob Mailbox auf Exchange, myTUM-Mailserver oder externem Mailserver liegt
  - freie Wahl einer zusätzlichen Weiterleitung
- Forwarder wird Schaltzentrale
  - adress- und nicht domain-bezogenes Routing an gewünschten Message-Store
  - Ausführung der Weiterleitungen an externe Adressen
  - Implementation komplex wegen Exchange

Fazit (1)

- Anti-Spam und Anti-Viren-Funktionalität wurde erfolgreich implementiert
- zahlreiche Rückschläge auf dem Weg zu einem zentralen Mail- bzw. jetzt Groupware-Service
- dadurch ursprüngliches Ziel – Migration der vielen virtuellen und lokalen Mailserver auf den zentralen – nur zu einem geringen Teil erreicht

Fazit (2)

- Forwarder seit gut einer Woche in Betrieb
- Exchange nach Voll-Sync zwischen Meta-Directory und Active Directory/Exchange seit gestern Nachmittag in Produktionsbetrieb
- Ausblick
  - Implementation der Administrationsoberfläche zur Verwaltung von Ressourcen
  - Erstellung und Verwaltung von Gruppen