Electronic Mail – was gibt's Neues?

Electronic Mail ist ja eigentlich ein alter Hut, sollte man meinen, so daß es keine Neuerungen oder Änderungen geben dürfte.

Das wäre auch fast richtig, wenn sich das Mailing nicht so sprunghaft zum Massenkommunikationsmedium entwickeln würde, einschließlich der zunehmenden kommerziellen Nutzung.

Die verstärkte Nutzung von E-Mail ist auch bei uns am Rechenzentrum deutlich spürbar. Das hat natürlich Auswirkungen auf die eingesetzte Rechentechnik, die mit einer steigenden Nutzeranzahl und den wachsenden Mailmengen (bedeutet auch Speicherkapazität) fertig werden muß. Dementsprechend wird der Popserver durch die Abfragen der Mailboxen stark frequentiert. Es ist also auch eine Frage der Quantität, die die Stabilität und Qualität eines Dienstes – hier also Electronic Mail – beeinflußt. Herr Sittel zeigt in seinem Artikel zum Thema DCE solche Zusammenhänge ebenfalls auf. Wir versuchen deshalb am Rechenzentrum, durch organisatorische und investive Maßnahmen die Qualität von angebotenen Diensten, wie z. B. Electronic Mail, zu halten und zu verbessern. Dabei sind Ausfälle leider nicht völlig auszuschließen, wie uns erst kürzlich die Erfahrung mit unserem hardwaremäßig erneuerten Mailserver lehrte.

Ferner sind verschiedene Dienste sehr eng verquickt bzw. führen nur in Kombination zum Erfolg. Ein typischer Ausgangspunkt in Problemfällen ist die Mitteilung „Meine E-Mail geht nicht mehr". Die Fehlermöglichkeiten reichen dann von Problemen auf dem eigenen PC, bei der telefonischen Einwahl bzw. im Campusnetz, beim Einloggen (Account und Paßwort) bis zum Mailserver selbst. Das Lesen oder Verschicken von E-Mail ist für den Nutzer eine simple Angelegenheit, in Wirklichkeit aber ein ziemlich komplexer Vorgang.

Neue Struktur des Maildienstes

Eine Prämisse für die Organisation des Maildienstes besteht darin, diesen von anderen zu entkoppeln, so daß Ausfälle anderer Dienste oder Ressourcen den Maildienst möglichst nicht beeinträchtigen.

Dabei ergeben sich durch die Arbeitsweisen der Nutzer durchaus unterschiedliche Varianten. Stellen Sie sich vor, Sie benutzen eine Telnet-Verbindung zu einem unserer Rechner, um auf diesem direkt mit den Tools elm oder mailx Ihre Mail zu lesen. Für das Einloggen ist dabei das Home-Verzeichnis, das per NFS von einem Fileserver bereitgestellt wird, erforderlich. Ist diese Ressource gerade nicht verfügbar, können Sie nicht arbeiten, obwohl die Mailbox erreichbar wäre.

Holen Sie sich aber Ihre Mail mit einem POP-basierten Mailtool (z. B. Eudora) ab, dann merken Sie davon gar nichts, weil der Popserver inzwischen von den Home-Verzeichnissen entkoppelt ist. Aber kein Vorteil ohne Nachteil: Die nutzergesteuerte Mailweiterleitung per „.forward-File", das üblicherweise im Home-Verzeichnis liegt, ist erst einmal nicht möglich. In der Vergangenheit führte nämlich genau diese Konstellation bei einem Ausfall des Fileservers mit den Home-Verzeichnissen auch zum Ausfall des Maildienstes. Dazu kommt, daß weniger als ein Prozent unserer Nutzer diese Möglichkeit nutzen, aber alle vom Ausfall betroffen waren, wenn der Mailserver auf die Verfügbarkeit der „.forward-Files" warten mußte.

Im März haben wir den Mailserver auf eine neue Hardwarebasis (UltraSPARC, 200 MHz, 256 Mbyte RAM) gestellt. Die Mailboxen befinden sich in einem RAID-5-System, das die Datenspeicherung über sechs Festplatten streut und selbst bei einem Ausfall einer Platte den Dateninhalt rekonstruieren kann. Insofern haben wir die Datensicherheit der Mailboxen unabhängig von den weiterhin durchgeführten Datensicherungen erhöht. Insbesondere kann mit dem RAID-5-System der aktuelle Zustand rekonstruiert werden, die Wiederherstellung der Mailboxen von einer Kopie zum Zeitpunkt „x" kann die inzwischen erfolgten Veränderungen nicht berücksichtigen. Ob das RAID-5-System das Versprochene im Ernstfall leistet, werden wir sehen.

Auf der gleichen Maschine laufen auch der POP- und der IMAP-Server, die damit direkten Zugriff zu den Mailboxen haben. Die bereits angesprochenen „.forward-Files" werden ebenfalls in einem Filesystem des Mailservers bereitgestellt. Die Verbindung zu diesem ursprünglich im Home-Verzeichnis des Nutzers liegenden File wurde dort durch einen sogenannten „symbolischen Link" ersetzt, so daß bei Bedarf diese Möglichkeit der Mailweiterleitung weiterhin nutzbar ist. Nebenbei gesagt, das wird oft fehlerhaft angewendet, so daß Mailverluste für den Nutzer die Folge sind. (vgl. URL: http//www.hu-berlin.de/rz/comm/mail/forward.html)

In der Abbildung ist das funktionelle Zusammenspiel der am Maildienst beteiligten Komponenten schematisch dargestellt. Für die Konfiguration von Mailtools, die mit dem POP- oder IMAP-Server zusammenarbeiten, sind nur wenige Angaben erforderlich, die ich hier noch einmal nennen möchte.

Eudora verlangt z. B. folgende Angaben:

POP account
Mit dem Eintrag

account@popserv.rz.hu-berlin.de

legt man fest, daß die Mail mittels POP-Protokoll vom POP-Server abgeholt werden soll. Der Account dient

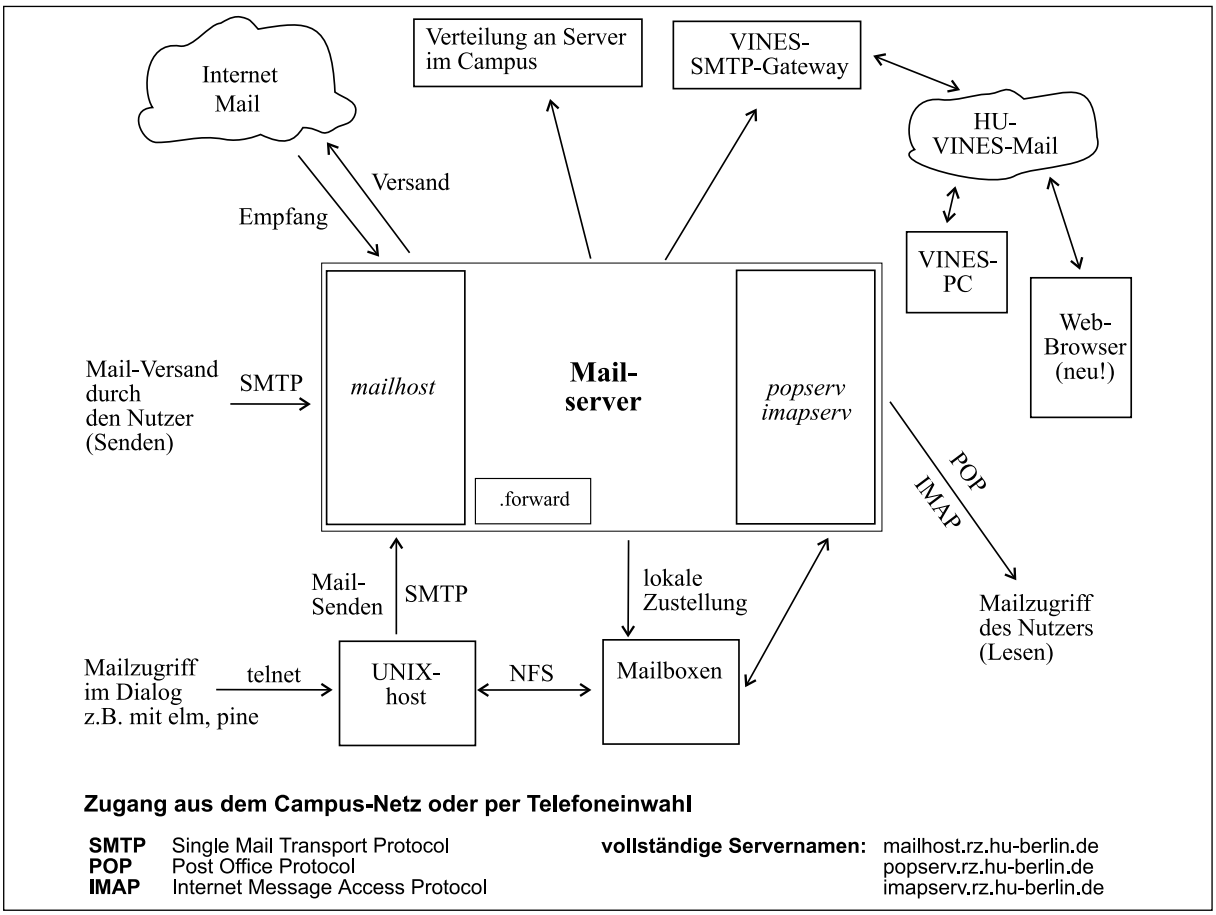

Abb.: Organisation des Maildienstes

zur Identifizierung des Nutzers und seiner Mailbox. Analog gibt man imapserv an, wenn ein Mailtool das IMAP-Protokoll verwendet.

Real Name
Hier kann der persönliche Name angegeben werden. Dieser wird dann in einer abgehenden Mail als Kommentar mitgeschickt.

Return address
Das ist ein sehr wichtiges Feld, hier entscheidet der Nutzer, ob er Antworten auf seine Mails „erhalten möchte“!

In das Feld gehört die korrekte eigene Mailadresse, die als Absender mitgeschickt wird. Für Nutzer des Rechenzentrums kann das prinzipiell folgender Eintrag sein

account@rz.hu-berlin.de

bzw. für unsere Studenten

account@student.hu-berlin.de

Darüber hinaus hat jeder Nutzer auch eine „schöne“ Mailadresse, über die er einmalig bei Eröffnung seines Accounts informiert wurde. Sie wird aus den Namensbestandteilen des Nutzers gebildet, im einfachsten Fall ist es

vorname.nachname@rz.hu-berlin.de

Diese Adresse wird auch als Alias bezeichnet und ist dem Account zugeordnet.

SMTP
Eine Mail wird unter Nutzung des Simple Mail Transport Protocol (SMTP) an einen „zuständigen“ Mailserver geschickt, der sich dann um den Weitertransport kümmert. Es ist sozusagen der Sammelbriefkasten und lautet für unsere Nutzer

mailhost.rz.hu-berlin.de

Nutzer von MS Outlook unter Windows 95 finden bei der Konfiguration von „Internet E-Mail – SMTP“ unter der Rubrik „Server“ die Begriffe **Posteingang** (POP3) und **Postausgang** (SMTP) für die Angabe der entsprechenden Servernamen.

Der noch fehlende Account wird unter der Rubrik „Anmelden als:“ nach dem Stichwort „Kontoname“ angegeben.

Andere Mailtools, z. B. in Netscape, benötigen diese Angaben ebenfalls, benutzen aber z. T. nur andere Bezeichnungen.

Mailmißbrauch

Zurück zu unserem Mailserver – die veränderte Konstellation ist nur ein Aspekt der Sicherheit. Die Angriffe auf Mailserver im gesamten universitären

Bereich nehmen zu. In den RZ-Mitteilungen Nr. 15 (URL: http/www.hu-berlin.de/rzmit/rzm15/9.html) hatte ich in meinem Artikel „Electronic Mail – Gefahr für die Sicherheit“ auch den Mailmißbrauch angesprochen. Das „Spamming“ genannte massenhafte Verschicken von E-Mail zweifelhaften Inhalts oder das Posten in mehrere Newsgruppen ist nach wie vor aktuell. In diesem Zusammenhang werden auch die Begriffe UCE (Unsolicited Commercial E-Mail) oder allgemeiner UBE (Unsolicited Bulk E-Mail) benutzt.

Solche Mails, versehen mit umfangreichen Adreßlisten, werden von den sogenannten Spammern auf möglichst vielen Mailservern eingeliefert, die in ihrer Standardkonfiguration die Mail auch weltweit zustellen (third party relaying genannt). Damit mißbraucht der Spammer bewußt Server- und Netzkapazität, der adressierte Nutzer hat bei telefonischer Abfrage seiner Mailbox mit einer längeren Verbindungsdauer zu rechnen, letztlich also auch mit höheren Telefonkosten. Die Administratoren/Postmaster der mißbrauchten Mailserver haben anschließend eine Vielzahl von Beschwerden zu bearbeiten. Außerdem kann der Mailserver auf eine „schwarze Liste“ kommen, die allen als Informationsquelle offensteht. Eine Einrichtung im Internet kann dann z. B. den Mailaustausch mit diesen „geächteten“ Servern völlig unterbinden! Als Betreiber eines Mailservers muß man sich also darum kümmern.

Zum einen wollen wir verhindern, daß Mailserver in unserer Domain hu-berlin.de als „third party relay“ benuzt werden, zum anderen müssen wir auch den Mißbrauch durch unsere eigenen Nutzer verhindern.

Darum führen wir derzeit in Zusammenarbeit mit den DV-Beauftragten und Betreibern von Mailservern mehrere Maßnahmen durch bzw. bereiten sie vor:

- Einsatz der neuesten Sendmail-Version (8.8.8), die z. B. Möglichkeiten zur Unterbindung des „third party relaying“ enthält.
- Einschränkung der Anzahl der Mailserver, die direkten Kontakt mit dem Internet haben.
- Unterbindung des direkten Mailaustauschs (Senden und Empfangen) mit dem Internet für alle anderen Rechner unserer Domain.
- Überprüfung der Absenderadresse auf ihre Korrektheit, d. h. es muß eine gültige Adresse innerhalb der Domain hu-berlin.de sein.
- Die IP-Adresse von Rechnern in unserem Netz muß im Domain Name Service (DNS) – das „Adreßbuch“ der Rechner im Internet – registriert sein, was über die DV-Beaufragten realisiert wird.

Sie können sich sicher vorstellen, daß weltweit viele Administratoren und betroffene Nutzer damit beschäftigt sind, Möglichkeiten zu finden, um diesen Mißbrauch einzudämmen. Einige Provider stellen inzwischen bei nachgewiesenem Spamming dem Verursacher die Unkosten in Rechnung, wenn er zum eigenen Kundenkreis gehört. Außerdem gibt es auch erste juristische Ansätze.

Eingesetzte Gegenmaßnahmen bzgl. des „third party relaying“ haben aber auch Nebenwirkungen. Beispielsweise kann ein Dienstreisender aus dem Netz seiner Gastuniversität seine Mailbox bei uns abfragen, er kann aber aus diesem „fremden“ Netz keine E-Mail an Dritte über unseren mailhost.rz.hu-berlin.de verschicken. Ausnahmen sind in Einzelfällen möglich. In der Regel ist aber der Mailhost im dortigen Netz für den Mailversand zu nutzen. An dieser Stelle kann ich nur auf Ihr Verständnis für diese Maßnahmen hoffen.
Falls Sie in das Thema einsteigen möchten, hier zwei URL:
http://www.stud.uni-hannover.de/news/de.admin.net-abuse.mail.html oder
http://math-www.uni-paderborn.de/~axel/BL/blacklist.html

Und sonst?

Vielleicht ist Ihnen in der Abbildung aufgefallen, daß es eine neue Zugriffsmöglichkeit auf Mailboxen im Banyan VINES gibt? Sie können aus modernen Web-Browsern heraus in unser VINES-Netz „einsteigen“ und sich Ihre VINES-Mailbox öffnen. Die Firma Banyan hat mit dem Produkt *Banyan Intranet Connect* eine entscheidende Lücke geschlossen. Wenn Sie interessiert sind, lesen Sie den Artikel von Herrn Naumann in diesem Heft.

Erinnern Sie sich noch an unser Heft Nr. 12, das dem Mailing gewidmet war? (URL: http/www.hu-berlin.de/rz/rzmit/rzinhalt.html)

Wir hatten versucht, Empfehlungen für verschiedene Nutzungsformen von E-Mail bei uns zu geben. VINES-Mailboxen sind nunmehr auch über externe Zugangswege gut nutzbar, zumal sich inzwischen bei den Web-Browsern ebenfalls viel getan hat. Probieren Sie es aus!

Burckhard Schmidt