UNIVERSITÄTS-
RECHENZENTRUM

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Verwaltungs- und Benutzungsordnung

Universitätsrechenzentrum

Verabschiedet vom EDV-Ausschuss am 08. November 1999.

E-Mail Firewall für die Universität Heidelberg

Wie bekannt, fand am 8.9.1999 eine sogenannte "SPAM-Attacke" auf die Universität statt, d.h. es wurden ungeschützte Mailsysteme innerhalb der Universität Heidelberg missbraucht zum Verschicken von Werbemüll (*spam mail*) mit dem Effekt, dass die Universität Heidelberg dann als Absender des Werbemüll erscheint.
Schon vor diesem Zeitpunkt hatte das Universitätsrechenzentrum ein Mail-Firewall in Arbeit, das durch diese Spam-Attacke eine traurige Aktualität erfahren hat und nun eine höhere Priorität erhält. Im folgenden wird unter dem Titel **Mail-Firewall** der Schutz gegen Werbemüll und Missbrauch von Mailsystemen allgemein beschrieben. Im Anschluss daran wird unter **Implementierung** auf die aktuellen und geplanten Aktionen eingegangen.

Mail-Firewall gegen Mailmissbrauch (*Spam, Spam Relay*)

Im Internet ist ein rapides Ansteigen von Werbemüll (*Spam*) und damit einhergehend ein Missbrauch fremder Mailsysteme zur Verteilung von Werbemüll (*Spam Relay*) zu beobachten. Da beiden Missbrauchsarten derzeit nur schwer juristisch beizukommen ist, muss man das Problem technisch in den Griff bekommen.
Dabei stellt sich die Frage, ob jeder der mehr als 700 Mailserver in der Universität einzeln abgesichert, oder der Campus insgesamt durch zentrale Filterfunktionen (*Mail Firewall*) vor *Spam* und *Spam Relay* geschützt werden soll. Da es in der Vergangenheit trotz der Richtlinien im zentralen Versorgungskonzept immer wieder Probleme bei den dezentralen Mailservern in den Instituten gab (z. B. veraltete Software oder personelle Probleme bei der Betreuung der Mailserver), stellt sich eine zentrale Lösung des Problems als einzig sinnvolle dar.

Ziel eines zentralen Mail-Firewalls

Durch einen zentralen Mail-Firewall lassen sich

- sowohl alle dahinter liegenden Mailsysteme innerhalb der Universität Heidelberg gegen Missbrauch zur Verteilung von Werbemüll (*Spam Relay*) schützen
- als auch gegen Werbemüll (*Spam*) selbst durch entsprechende Filter bei der Annahme von Mail.

Dadurch werden vor allem die Institute entlastet, die eigene Mailserver betreiben und Probleme bei der Wartung der Mailsysteme haben, aber auch die vielen Einzelpersonen, die z. B. Linux auf ihrem PC und damit evtl. unabsichtlich einen Mailserver installiert haben.

Wie funktioniert ein zentraler Mail-Firewall?

Über den zentralen Mail-Firewall muss alle eingehende und alle ausgehende Mail der Universität Heidelberg geleitet werden:

- Alle eingehende Mail wird durch entsprechende Eintragungen (im *Nameservice* und im Eingangs-Router) zum zentralen Mail-Firewall umgeleitet, der sie dann an weitere Mailserver in den Instituten weiterleitet.
- Umgekehrt muss alle ausgehende Mail über den zentralen Mail-Firewall ins Internet geschickt werden, sowohl von den Mailservern in den Instituten als auch von den Mail-Clienten auf den PCs.

Alle Mails laufen dann über den zentralen Mail-Firewall, und der Mailport (Port 25) aller anderen Rechner der Universität ist dann von außerhalb nicht mehr ansprechbar.

Eingehende Mail

Im *Nameservice* leiten sogenannte *MX-records* ordnungsgemässe Mail für eine *Subdomain* `institutskürzel.uni-heidelberg.de` zum zentralen Mail-Firewall um, während illegale Mail, die sich nicht an die Umleitung halten will, im Router gefiltert wird.
Bei der eingehenden Mail im Mail-Firewall (vom Internet oder aus der Universität) wird geprüft, ob der Absender oder einer der Empfänger innerhalb der Universität Heidelberg ist - wenn nicht, wird der Empfang dieser Mail abgelehnt. Danach wird geprüft, ob der abschickende Rechner in einer "schwarzen Liste von Rechnern (*Spam Filter*)" steht - wenn ja, wird ebenfalls der Empfang der Mail abgelehnt.
Da die zentralen Spam Filter nur grob sein können, bleibt es den Instituten überlassen, diese auf eigenen Mailservern zu verschärfen - z. B. kann das URZ nicht zentral die Annahme von Mail von *hotmail.com* verbieten, da mit einigen Personen dort "normal" kommuniziert wird, ein Institut jedoch kann für sich entscheiden, von niemandem bei *hotmail.com* Mail annehmen zu wollen.
Sind alle Prüfungen erfolgreich bestanden, wird die Mail an einen Mailserver im Institut weitergeleitet. Dabei ist zu beachten, dass es pro Institut - genauer pro *Subdomain* `institutskürzel.uni-heidelberg.de` - **nur einen** Mailserver geben kann,

an den die Mail weitergeleitet wird. Bei Bedarf kann dann dieser Mailserver die Mails im Institut an weitere Mailserver verschicken.

Ausgehende Mail

Wie oben beschrieben soll alle ausgehende Mail über den zentralen Mail-Firewall geleitet werden. Dabei muss man unterscheiden zwischen Mailservern und Mail-Clienten.

- Für die ausgehende Mail müssen die Betreiber von dezentralen Mailservern lediglich definieren, dass die Mail über ein sogenanntes Mailrelay verschickt wird - dies geschieht für
  - Unix sendmail im File sendmail.cf über das DS Makro
  - Novell Mercury Mailer im File mercury.ini in der Sektion [Mercury] durch Angabe einer Relay-Zeile
- Bei Mail-Clienten (Netscape, Outlook Express usw.) ist durch die Angabe von
- SMTP-Server, Server für ausgehende Mail oder ähnliche Einträge

  dafür zu sorgen, dass ein Mailrelay innerhalb der Universität Heidelberg angegeben wird. Dies ist normalerweise der Rechner, von dem man die Mail liest (POP/IMAP-Server).

Implementierung

Aufgrund der aktuellen SPAM-Attacke ist der Mailport (Port 25) bereits nicht mehr allgemein nutzbar, sondern nur noch von Rechnern, die dem URZ gemeldet und in eine Ausnahmeliste aufgenommen wurden. Langfristig soll diese Ausnahmeliste wieder aufgegeben werden und nur noch Mail vom zentralen Mail-Firewall aus dem Internet angenommen bzw. ins Internet geschickt werden.

Erste Tests mit ungeschützten Mailsystemen waren bereits erfolgreich, sodass wir hier schon stichwortartig beschreiben können, welche Maßnahmen bei den Mailservern und Mail-Clienten zu ergreifen sind. Als Mail-Firewall wird der Rechner mit den Namen **relay.uni-heidelberg.de** verwendet. Novell Mercury Mailer unterstützen keine IP-Namen und benötigen daher die IP-Adresse 129.206.100.212 .

Implementierungsbeispiele

(wurden in einen eigenen Teil verlagert, um die Pflege und Fortschreibung zu erleichtern)

Mit diesem Mail-Firewall kann das Rechenzentrum als Diensteanbieter für alle Institute der Universität einen nach dem Stand der Technik aktuellen und vor Spam-Weiterverbreitung gesicherten Maildienst anbieten.