Policy für die zentralen Mailrelays des RZ

Stand:18.07.2008 *Thomas.Eiler@RZ.Uni-Passau.De*

In diesem Beitrag werden die Regeln beschrieben, nach denen die zentralen Mailrelays des RZ betrieben werden.

Inhalt

Einleitung

In diesem Dokument wird das Verhalten der zentralen Mailrelays des RZ beschrieben, so wie es von außen von anderen Mailservern und unseren Kunden festgestellt werden kann. Dies umfasst alle Regeln und Konfigurationsdaten, die eine Wirkung auf die Außenwelt haben.
Als zentrales Mailrelay wird derzeit nur der Rechner

- ***mail.rz.uni-passau.de***

eingesetzt. Aus der Sicht der Mailserver an der Uni wird *mail.rz.uni-passau.de* sowohl für **ankommende/empfangene** E-Mails genutzt (MX-Records im DNS), kann aber auch von den Mailclients und Mailservern als Forwarder verwendet werden, d.h. also für **abgehende/gesendete** E-Mails (wie z.B. derzeit beim NOVELL-Mailer).
Die Regeln und Konfigurationseinstellungen für die zentralen Mailrelays des RZ sind in 3 Teile gegliedert:

- Empfang von E-Mails
- Verarbeitung von E-Mails

- Versand von E-Mails

Dabei sind die Begriffe Empfang und Versand von E-Mails immer aus der Sicht der Mailrelays beschrieben. Das bedeutet, egal ob eine E-Mail von einem Mailserver oder -client aus dem Internet empfangen oder in selbiges geschickt wird, muss die E-Mail grundsätzlich zuerst auf dem Mailrelay empfangen, dann verarbeitet und anschließend wiederum versand werden, sofern die Mailrelays bei der Übertragung der E-Mail eine Rolle spielen, d.h. die Mail dort überhaupt vorbeikommt.
Jede Regel oder Konfigurationseinstellung wird durch eine ***Policy*** beschrieben. Jede Policy ist in mehrere Punkte gegliedert:

- **Ziel**: Was soll mit dieser Policy erreicht werden (Kurzfassung).
- **Zielgruppe**: Wen betrifft diese Policy besonders, hauptsächlich Administratoren von anderen Mailservern, oder jeden einzelnen unserer Kunden selbst.
- **Beschreibung**: Was soll mit dieser Policy erreicht werden (Langfassung)? Wie sieht die Implementation aus, welche Algorithmen werden verwendet.
- **Auswirkungen**: Welche Auswirkungen hat diese Policy auf die Zielgruppe, welche Aktionen muss die Zielgruppe durchführen.
- **Gültig ab**: Ab welchem Zeitpunkt tritt die Policy in Kraft.

Empfang von E-Mails

Allgemeines

Dieser Abschnitt beschreibt die Policies, die den Empfang von E-Mails durch die Mailrelays des RZ beeinflussen. Dies betrifft wie oben schon erwähnt sowohl E-Mails von Mailservern aus dem Internet als auch von Mailservern aus dem lokalen Netz. Durch spezielle Regeln werden diese beiden Gruppen aber unterschiedlich behandelt.

Geordnet sind die Policies nach den einzelnen Schritten im Ablauf der Übertragung einer E-Mail von einem Rechner auf den anderen:

- Aufbau der TCP/IP-Verbindung
- Aufbau der auf die TCP/IP-Verbindung aufsetzenden SMTP- bzw. ESMTP-Verbindung (Austausch des Protokollelements *HELO* bzw. *EHLO*)
- Übertragung einer oder mehrerer E-Mails, wobei sich diese jeweils wiederum in 3 Teile aufteilt:
    - Absender der E-Mail (Originator, Protokollelement *Mail From*)
    - ein oder mehrere Empfänger (Recipient, Protokollelement *RCPT To*)
    - Übertragung des eigentlichen Inhalts der E-Mail (Protokollelement *Data*)

Absender und Empfänger aus dem SMTP- bzw. ESMTP-Protokoll werden auch als der Umschlag der E-Mail bezeichnet. Diese sind nicht mit dem Absender und den Empfängern aus dem ersten Teil des Inhalts der E-Mail, dem sogenannten Header zu verwechseln. Diese Adressen können ganz andere sein.

Zum Schluss werden die Policies aufgeführt, auf die sich andere Policies abstützen.

Vertrauenswürdige Mailserver

Ziel

Ist ein Rechner ein *vertrauenswürdiger Mailserver*, so betrachten die zentralen Mailrelays diesen Rechner als einen ihrer Kunden. Für diese Rechner gelten daher andere Regeln beim Empfang und Versand von E-Mail als bei einem Rechner, der nicht zu den *vertrauenswürdigen Mailservern* gehört.

Zielgruppe

alle

Beschreibung

Um eine E-Mail über eines der zentralen Mailrelays zu schicken, baut ein Mailserver zuerst eine TCP/IP-Verbindung zu einem der Mailrelays auf. Dabei wird unter anderem die IP-Adresse des sendenden Mailservers an den MTA auf dem Mailrelay übergeben. Für diese IP-Adresse versucht das Mailrelay mit einer *Reverse Mapping* Abfrage beim DNS den zugehörigen Domainnamen herauszubekommen.

Ist der entsprechende Nameserver nicht erreichbar (errno=146, h_errno=2) bzw. tritt ein anderer temporärer Fehler bei der DNS-Abfrage auf, so kann nicht entschieden werden, ob der Mailserver zu den vertrauenswürdigen Servern gehört oder nicht. Aus diesem Grund wird die TCP/IP-Verbindung zurückgewiesen.

Bei Erfolg wird der Domainname, ansonsten die IP-Adresse in der untenstehenden Tabelle gesucht. Wird sie gefunden, so gehört der Rechner zu den *vertrauenswürdigen Mailservern*. Ein '*' in der Tabelle bedeutet, dass alle Subdomains bzw. alle Rechner aus diesem Netz vertrauenswürdig sind.

vertrauenswürdige Domainnamen, IP-Adressen
*.uni-passau.de
132.231.*

Auswirkungen

Die Eigenschaft *vertrauenswürdiger Mailserver* wird von einer Reihe anderer Policies benutzt, um zu entscheiden, welche Teilregel beim Empfang von Mails anzuwenden ist:

- *Relay-Blocking*

Gültig ab

12.11.1997

Größe einer Mail

Ziel

E-Mails werden nur bis zu einer Größe von 30.000.000 Bytes angenommen. Dies gilt aus der Sicht eines Mailclients oder -servers sowohl für den Empfang als auch für den Versand von E-Mails.

Zielgruppe

alle

Beschreibung

Die Einschränkung der Größe der übertragenen E-Mails hat sich aus zwei Gründen als notwendig erwiesen:

- Die Protokolle *SMTP* bzw. *ESMTP* sind keine Filetransferprotokolle wie z.B. *FTP*, da sie nicht für die Übertragung großer Datenmengen optimiert sind. Kommt es bei einer Übertragung zusätzlich noch zu Verbindungsabbrüchen, so gibt es keinen Mechanismus, um bei einem erneuten Verbindungsaufbau die Übertragung an der Stelle beginnen zu lassen, wo sie beim Abbruch der Verbindung geendet hat. Somit müssen alle Daten von neuem übertragen werden.
- Es kommt immer wieder vor, dass ein Programm 'Amok' läuft und sehr große Mailfiles (z.B. Logfiles) erzeugt, die dann oft noch an eine Reihe von Personen geschickt werden. Oder jemand stößt, ohne sich dessen bewusst zu sein, die Übertragung einer sehr großen Datei an.

Diese Probleme führten in der Vergangenheit immer wieder dazu, dass die Ressourcen der beteiligten Mailserver bis an die Grenze beansprucht wurden, und es zu Problemen beim Austausch regulärer E-Mails kam.

Bei der Überprüfung der Nachrichtengröße sind zwei Fälle zu unterscheiden:

- Der sendende Mailserver benutzt das Protokoll ESMTP. In diesem Fall schickt das Mailrelay als Antwort auf den Verbindungsaufbau (Protokollelement *EHLO*) den Parameter *size* und die Angabe 30000000 zurück. Der sendende Mailclient oder -server weiß dann, ob die E-Mail von der Größe her übertragen werden kann oder nicht. Sollte sie zu groß sein, generiert er eine Fehlermeldung an den Absender der E-Mail.
- Der sendende Mailclient/-server hält sich nicht an obiges Verfahren und versucht die E-Mail trotzdem zu übertragen oder er verwendet das Protokoll *SMTP*. In diesem Fall schickt das Mailrelay, sobald die E-Mail die Größe von 30.000.000 Bytes überschreitet, die Fehlermeldung
  552 message size exceeds maximum message size
  und bricht die TCP/IP-Verbindung ab.

Die relevante Größe ist die Bruttogröße, d.h. die E-Mail mit der Transfer-Kodierung. Das bedeutet bei der Verwendung der Transfer-Kodierung *BASE64*, die in der Regel für Dateianhänge (Attachments) verwendet wird, dass die Netto-Größe bei ca. 20 MByte liegt.

Auswirkungen

Es können über die zentralen Mailrelays keine E-Mails größer als 20 MByte gesendet oder empfangen werden. Größere E-Mails müssen auf mehrere E-Mails aufgeteilt werden.

Gültig ab

01.01.2000 (10MB), 28.06.2006 (20MB)

Korrekte Syntax der Absende- und Empfangsadressen, DNS-Auflösung

Ziel

- Zurückweisung von E-Mails, die nach dem Eintreffen am Zielrechner nicht zugestellt werden könnten, wegen der syntaktisch falschen Empfangsadresse.
- Zurückweisung von E-Mails, an die keine Fehlermeldungen zurückgeschickt werden könnten, wegen der syntaktisch falschen Absenderadresse.
- Zurückweisung von E-Mails, an die keine Fehlermeldungen zurückgeschickt werden könnten, weil der Domainteil der Absenderadresse nicht im DNS auflösbar ist.

Zielgruppe

alle

Beschreibung

Es wird die Syntax der Adressen in den SMTP-Protokoll-Elementen *MAIL FROM* und *RCPT TO* überprüft. Dabei gelten die Regeln aus den Standards *RFC 821*, *RFC 952* und *RFC 1123*:

Die häufigsten syntaktischen Fehler sind

- Blanks in einer Mailadresse, insbesondere anstatt eines '.' oder vor/nach einem '.'
- das Zeichen '.' am Ende des linken Teils der Adresse direkt vor dem Zeichen '@'
- '.-' oder '-.' in der Domain
- Umlaut in der Adresse
- Teile, die der Adresse vorangestellt werden, aber nicht dazu gehören, wie SMTP:adresse oder mailto:adresse

Auswirkungen

Es wird so früh wie möglich eine Fehlermeldung generiert und zwar vom sendenden Mailserver. Dabei geht eine Kopie an den Postmaster des sendenden Rechners oder die Fehlermeldung landet direkt beim Absender. Damit hat der Absender viel schneller eine Reaktion und es kann ihm durch den Postmaster vor Ort viel eher geholfen werden.

Wird eine Mail mit syntaktisch falscher Absenderadresse erst angenommen und kann dann wegen einer falschen Empfangsadresse nicht weitergeleitet werden, so kann an den Absender keine Fehlermeldung geschickt werden. Solche Fehlermeldungen landen beim Postmaster der Mailrelays und werden dort halbautomatisch (über Filter) gelöscht.

Gültig ab

01.01.2000

Relay-Blocking

Ziel

Mit dieser Policy soll der Missbrauch der zentralen Mailrelays als Relay, insbesondere als Spam-Relay, ausgeschaltet werden.

Zielgruppe

alle

Beschreibung

Gehört ein Mailserver nicht zu den in der Policy *Vertrauenswürdige Mailserver* festgelegten Mailservern, dann wird eine E-Mail von den zentralen Mailrelays nur entgegengenommen, wenn Sie an Empfänger innerhalb der Uni adressiert ist, d.h. die Domain der Empfangsadresse muss zu den *akzeptierten Maildomains* gehören.

Überprüft wird die Adresse in jedem Protokoll-Element *RCPT-To*. Ist die Domain der Adresse eine der akzeptierten Maildomains, so wird die Mail akzeptiert. Ist sie dies nicht, so wird die Mail für diesen einen Empfänger mit der Fehlermeldung

551 Relay request denied

abgelehnt. Diese Überprüfung wird für jeden Empfänger der E-Mail durchgeführt. Wird keiner der Empfänger akzeptiert, so wird das Protokoll-Element *Data*, d.h. der Wunsch nun den Inhalt (Content) der E-Mail zu übertragen mit der Fehlermeldung

503 No valid recipients specified

abgelehnt.

Auswirkungen

Kunden, die über einen anderen Internet Service Provider (ISP) eine Verbindung zum Internet aufbauen - sie befinden sich damit ausserhalb der Uni -, können die zentralen Mailrelays des RZ nicht mehr für den Versand von E-Mail ins Internet benutzen. Sie müssen in diesem Fall die Mailrelays ihres ISPs verwenden.

Dies betrifft insbesondere diejenigen, die Wählzugänge anderer ISPs oder die Einwahlmöglichkeiten der Bürgernetze verwenden. Aber auch Studenten und Mitarbeiter aus dem Bereich der Uni, die als Gast an einer anderen Hochschule/Universität weilen und weiterhin die Mailrelays des RZ benutzt haben, müssen ihren Rechner, z.B. Notebook, umkonfigurieren.

Gültig ab

12.11.1997

Akzeptierte Maildomains

Ziel

Die *akzeptierte Maildomains* sind die Domains im lokalen Netz, für die die zentralen Mailrelays des RZ E-Mails entgegennehmen.

Zielgruppe

alle

Beschreibung

Ist die Domain einer Mailadresse in der Tabelle enthalten oder ist sie eine Subdomain einer Domain in der Tabelle, so gehört sie zu den akzeptierten Maildomains.

akzeptierte Maildomains
uni-passau.de

Auswirkungen

Die Eigenschaft *akzeptierte Maildomain* wird von einer Reihe anderer Policies benutzt, um zu entscheiden, welche Teilregel beim Empfang von Mails anzuwenden ist:

- *Relay-Blocking*

Gültig ab

12.11.1997

Verarbeitung von E-Mails

Allgemeines

Dieser Abschnitt beschreibt die Policies, die die Verarbeitung von E-Mails durch die Mailrelays des RZ beeinflussen.

Automatischer Virencheck von Emails

Ziel

Es soll an zentraler Stelle (Email-Ein/Ausgang) mit den aktuellsten Virensignaturen gescannt werden.

Zielgruppe

alle

Beschreibung

Jede Mail, die an den Mailrelays vorbeikommt, wird auf Viren untersucht. Falls ein Virus gefunden wird, wird der Absender der Nachricht durch eine automatisch erzeugte Mail hiervon unterrichtet und die entsprechende Mail gelöscht. Damit bemerkt ein Absender evtl. erst seinen Virusversand, kann sein System virenfrei machen und die Daten dann erneut schicken.

Bitte beachten Sie aber, dass damit keinesfalls alle Viren gefunden werden können, so dass Sie auch weiterhin sehr vorsichtig beim Umgang mit externen Daten (wie Emails, WWW-Seiten, Disketten etc.) sein müssen. Siehe hierzu auch die Sophos White Papers:
http://www.sophos.de/virusinfo/whitepapers
und die Sophos-Richtlinien für sicheres Computing:
http://www.sophos.com/virusinfo/articles/safehex.html

Die Virensignaturen des Scanners (Sophos) werden dabei automatisch stündlich aktualisiert.

Auswirkung

Emails, in denen Viren gefunden werden, werden an den Absender mit einer Fehlermeldung zurückgeschickt. Bei Viren, die bekanntermaßen den Absender fälschen, wird keine Fehlernachricht zurückgeschickt, um nicht unschuldige Dritte zu belästigen.

Gültig ab

23.10.2001

Nichtannahme von Spam-Mails

Ziel

Es werden alle eingehenden E-Mails bereits vor der Annahme automatisch auf Spam untersucht und bei Bestätigung sogleich an die absendende Stelle zurückgewiesen (reject).

Zielgruppe

Alle Personen, deren E-Mails beim Empfang über die Mailserver des RZ geleitet werden.

Beschreibung

Die Verteilung unerwünschter Werbe- und Massenmails, auch Spam genannt, hat sich mittlerweile zu einem ernsthaften und stark wachsenden Problem entwickelt. Durch das Speichern von Spam in den Mailkonten werden nicht nur Ressourcen im Netz und auf Servern unnötig belegt. Auch geht wertvolle Arbeitszeit durch die Kontrolle und das Löschen von Spam bzw. durch die ständige Pflege von Filterregeln zum Aussortieren derartiger E-Mails verloren. Beim Sichten von Spam besteht zudem die Gefahr, dass hierbei schädliche Programme eingeschleust werden und Rechner oder Netz lahm legen. Herkömmliche Server-Lösungen mit automatischer Markierung von Spam arbeiten zudem nicht immer befriedigend, wenn E-Mails fälschlich als Spam gekennzeichnet werden und daher in den meisten Fällen unbeachtet bleiben.

Um den bisherigen Aufwand wegen Spam deutlich zu reduzieren, wird künftig universitätsweit ein effizienteres Verfahren mit dem Produktnamen "eXpurgate" eingesetzt. Hierbei werden alle eingehenden E-Mails bereits vor der Annahme automatisch auf Spam untersucht und bei Bestätigung sogleich an die absendende Stelle zurückgewiesen. Ihr E-Mailkonto wird also nicht mehr mit Mails belastet, die als Spam eingeordnet werden können.

Auch die Spam-Erkennungsrate wird wesentlich höher als bisher - aber leider nicht 100% sein. Daher werden bei Ihnen auch weiterhin vereinzelt unerwünschte E-Mails (insbesondere solche mit gefälschten Adressen) ankommen, die Sie mit der notwendigen Vorsicht behandeln sollten.

Das System verspricht auch eine sehr niedrige Quote von fälschlich als Spam behandelten Mails, die aber wegen der Rückinformation über die Nichtzustellung an die Absender nicht spurlos verloren gehen.

Für dieses Vorgehen liegt die Zustimmung der Hochschulleitung vor.

Die Deaktivierung des Spam-Schutzes kann über folgendes WWW-Formular erfolgen:
https://www.rz.uni-passau.de/spamschutz.html

Weitere Hinweise zum Spam-Schutz findet man unter http://www.rz.uni-passau.de/anti-spam.html.

Auswirkungen

Ihr E-Mailkonto wird also nicht mehr mit Mails belastet, die als Spam eingeordnet werden können.

Gültig ab

18.07.2008

Versand von E-Mails

Allgemeines

Dieser Abschnitt beschreibt die Policies, die den Versand von E-Mails durch die Mailrelays des RZ beeinflussen. Die Beschreibung der entsprechenden Policies erfolgt zu einem späteren Zeitpunkt, da es bisher keine Einschränkungen gibt.

Zusätzliche Policies

Allgemeines

Diese Policies sind keine direkten Policies der zentralen Mailrelays, stehen aber in einem Zusammenhang mit diesen und sind aus diesem Grund hier aufgeführt.

Sperrung von Port 25 am Internet-Eingang ins lokale Netz

Ziel

Es soll für alle Mailserver im lokalen Netz der Uni verhindert werden, dass diese als Relay für Spam-Mails missbraucht werden können.

Zielgruppe

Administratoren der Mailserver

Beschreibung

Es wird der SMTP-Port 25 am Router zwischen Uni und Internet für SMTP-Verbindungen vom Internet in die Uni gesperrt. Damit sind die Mailserver der Uni nicht mehr direkt aus dem Internet erreichbar und können damit nicht mehr als Relay missbraucht werden. Dadurch ist es nicht mehr so dringend

sofort jeden einzelnen Mailserver selbst mit der neusten Mailsoftware zu versehen, die das Unterbinden des Relayings erlaubt.

Dadurch ist auch die Gefahr gebannt, dass der Ruf der Uni durch das Fehlverhalten einzelner Rechner geschädigt wird und die jeweilige gesamte Domain auf eine 'blacklist' kommt, womit der Austausch von E-Mails empfindlich gestört wäre.

Auswirkung

Damit weiterhin E-Mails mit dem Internet ausgetauscht werden können, gibt es eine Reihe von Mailrelays, die weiterhin E-Mails direkt aus dem Internet empfangen können.

Gültig ab

12.11.1997

Sperre des direkten Mailversands (mit SMTP)

Ziel

Es soll verhindert werden, dass von Rechnern innerhalb der Universität Emails mit enthaltenen Viren auf direktem Weg (unter Umgehung der Mailserver der Uni) nach außen verschickt werden können.

Zielgruppe

alle

Beschreibung

Es wird der SMTP-Port 25 am Router zwischen Uni und Internet für SMTP-Verbindungen von der Uni ins Internet gesperrt. Die registrierten Email-Server der Universität sind von der Sperre ausgenommen.

Mit dieser Blockade und der damit erzwungenen Mailauslieferung über die zentralen Mailserver wird eine automatische Ausbreitung der Viren weitgehend unterbunden. Dadurch ist auch die Gefahr gebannt, dass der Ruf der Uni durch das Fehlverhalten einzelner Rechner geschädigt wird und die jeweilige gesamte Domain auf eine 'blacklist' kommt, womit der Austausch von E-Mails empfindlich gestört wäre.

Auswirkung

Bei richtig konfigurierten Emailprogrammen ist keine Änderung nötig. Falls im Emailprogramm aber externe Mailserver als (ausgehende) Mailserver eingetragen sind (z.B. Web.de, GMX, Hotmail etc.), muss stattdessen der Server „mail.rz.uni-passau.de“ oder ein anderer freigeschalteter interner

Mailserver verwendet werden.

Gültig ab

16.07.2003