Open-Source-Systeme in der Mailumgebung am USZ

Adrian Senn

Universitätsspital Zürich

Einleitung

Das Universitätsspital Zürich (nachfolgend als USZ abgekürzt) betreibt seit längerer Zeit in der Firewall-Umgebung einige auf dem Open-Source-Betriebssystem Linux basierende Systeme.

Die Vorgaben waren, mit einfachen Mitteln eine gut funktionierende Umgebung aufzubauen. Neben den eigentlichen Firewall-Knoten, die mit einem RedHat Linux laufen, werden Mailgateways, http-Virenscanner, http-Proxyserver und Reverse-Proxyserver unter der Linux-Plattform betrieben. Teilweise laufen darauf aber kommerzielle Programme, die Linux als Plattform verwenden.

Wie auch in anderen Betrieben wird das Spam- und Viren- (bzw. Wurm-)problem immer grösser, und von den Kunden wird diesem Umstand auch eine grössere Aufmerksamkeit zugemessen. Dies führte nun dazu, dass am USZ der Wunsch nach einem effektiveren Filter grösser wurde.

Im folgenden Artikel soll vor allem die Mail-Umgebung für die Kommunikation nach aussen beschrieben werden.

Beschrieb der Umgebung

Im internen Netz wird seit einigen Jahren eine eigenständige Exchange-Umgebung betrieben. Damit die Kommunikation über die Firewall-Umgebung bewerkstelligt werden kann, sind diverse Mailgateways (sogenannte message transfer agents [MTA]) dazwischengeschaltet, die diverse Funktionen übernehmen.

Mit dem Aufbau der Firewall-Umgebung wurde in dieser ein Virenscanner für das Mailscanning eingehängt. Dieser basiert momentan auf einem Windows-Server und als Virenscanner wird ein Produkt von TrendMicro (Viruswall) verwendet. Gegenwärtig sind wir dabei, diesen Server durch eine Linux-basierte Plattform zu ersetzen.

Als externer Mailgateway diente lange Zeit ein Linux-Server, auf dem Sendmail als MTA im Einsatz war.

Überlegungen

Der Funktionsumfang auf der TrendMicro-Viruswall lies immer mehr zu wünschen übrig. So konnte keine schnelle Analyse der Virenmeldungen durchgeführt werden.

Ebenso konnte nur mit simplen Mitteln eine Spam-Filterung vorgenommen werden.

Auf dem externen MTA wurden gewisse Verbindungen von potentiellen Spam-Sendern schon seit längerem durch DNS-basierte Blacklists blockiert.

All diese Mechanismen wurden aber immer ungenügender, so dass von diversen Seiten her der Wunsch kam, einen besseren Spam- und Virenfilter zu implementieren.

Aufgrund privater Vorkenntnisse fiel die Wahl auf eine Open-Source-Scanengine mit dem Namen Mailscanner [1]. Bei dem Mailgateway (MTA) wurde ein Wechsel auf Postfix [2] in Erwägung gezogen. Sendmail bietet einen sehr grossen Funktionsumfang, ist aber aufgrund seines Aufbaus nicht immer trivial zu handhaben.

Postfix weist einen ähnlichen Funktionsumfang auf, bietet aber im Aufbau weniger Anlass zu Risiken als dies bei bestimmten Sendmailversionen der Fall ist.

Aufbau des externen Gateways

Als Hardwareplattform werden zwei HP DL 380 G3 verwendet. Es handelt sich um ein System mit einem 3-Ghz-Intel-Prozessor. Als Speicher wurden 1 GB Ram eingebaut. Diese werden soweit identisch aufgebaut, und einer bildet das Test- und Ausfallsystem für den produktiven Server. Als Betriebssystem wird Suse Linux Enterprise 9 verwendet. Von HP gibt es Hardwaremonitoringtools, die aber nur kommerzielle Linux-Versionen unterstützen.

Kontaktadresse:
Adrian Senn
UniversitätsSpital Zürich
Zentrale Informatik
Netzwerkgruppe

E-Mail: adrian.senn@usz.ch

Grundsätzlich läuft die weiter beschriebene Mail-Umgebung auch auf anderen Linux-Derivaten. Je nach dem sind gewisse Konfigurationen in gewissen Details anders.

Die Betriebssystem-Umgebung wurde mit den minimalst nötigen Software-Paketen installiert. So wurde auf eine Installation der X11-Umgebung verzichtet, da diese für den Betrieb als Mailserver nicht nötig ist.

Bei Postfix (MTA) wurde nicht die im Paket vorhandene Version verwendet, sondern selber kompiliert, da es so einfacher ist, auf eine neuere Version zu aktualisieren.

Für Mailscanner existieren fertige RPM-Pakete, die von der Mailscanner-Webseite runtergeladen werden können.

Die Umgebung von SpamAssassin [3] wurde wiederum selber kompiliert, damit auch hier die aktuellen Versionen verwendet werden können. SpamAssassin verwendet diverse weitere Werkzeuge zur Erkennung von Spam, die separat installiert werden müssen. Die Installation dieser Pakete ist im Readme von SpamAssassin gut beschrieben.

Zur Systemüberwachung wurde daneben noch HotSaNIC [4] für die Serverüberwachung und Mailscanner-mrtg [5] für das Monitoring des Mailverkehrs installiert.

Installation von Postfix

Die Installation der Postfix-Binaries erfolgte gemäss den Angaben der Installationsanleitung. Für die Konfiguration wurden Beispiele aus dem Internet [6] verwendet und für die eigenen Mailing-Bedürfnisse angepasst.

Für die erste Spam-Abwehr werden einerseits DNS-basierte Blacklists (RBLs), eigene Blacklists und andererseits seit Ende 2004 auch Greylisting [7] eingesetzt.

Da die Mails ins interne Netz an die Exchange-Server weitergeleitet werden, auf denen sich dann die eigentlichen Postfächer befinden, kann Postfix keine lokale Kontrolle über die existierenden Benutzeraccounts durchführen.

Es gibt aber eine Funktion, in der eine Tabelle von Benutzern oder Domains ausgelesen werden kann, für die ein Relaying durchgeführt wird. Diese Tabelle wird durch ein LDAP-Script, das eine Abfrage auf dem Active Directory Service der Windows-Server macht, alle 6 Stunden durch einen Cron-Job aktualisiert. So ist sichergestellt, dass keine Mails an unbekannte Benutzeraccounts angenommen werden, die bei grossen Viren- oder Spam-Befall an nicht vorhandene Adressen die internen Systeme zusätzlich unnötig belasten.

Der Test der Mail-Umgebung mit Postfix sollte in erster Linie ohne die weiteren Spam-Filterfunktionen durchgeführt werden, damit die Analyse auf den eigentlichen Mailverkehr beschränkt werden kann.

Installation von Mailscanner

Wie schon erwähnt, können von Mailscanner vordefinierte Pakete verwendet werden. Neben dem in den SuSe- und RedHat-Umgebungen bekannte RPM-Paketformat existiert auch ein Debian-Paketmanager.

Die Installation von Mailscanner benötigt gewisse Zusatzpakete. Die meisten werden mitgeliefert. Wenn ein benötigtes bereits installiert ist, werden diese Teile nicht mehr installiert.

Damit Mailscanner funktioniert, ist Spam-Assassin nicht zwingend notwendig. Ebenso ist es nicht zwingend notwendig, einen Virenscanner zu installieren. Ohne diese beiden Module fehlen aber wichtige Funktionen, um einen Inhaltstest der Mails durchführen zu können.

Um die ersten Installationstests durchzuführen empfiehlt es sich aber, diese ohne diese beiden Dienste durchzuführen.

Installation von ClamAV

Als Virenscanner wurde auf dem externen Gateway der Open-Source-Virenscanner installiert. Dieser hat sich recht gut bewährt und erkennt die meisten aktuellen Würmer. Da die Mails intern (Viruswall und Exchange) von TrendMicro Virenscannern nochmals gescannt werden, ist die Erkennungsrate sehr gut.

Der Virenscanner wurde gemäss Dokumentation der ClamAV-Webseite [8] direkt kompiliert.

Installation von SpamAssassin

Der Spam-Filter SpamAssassin [3] wurde ebenfalls selber kompiliert. Damit möglichst viele Funktionen genutzt werden können, braucht es diverse Perl-Module, die noch installiert werden müssen. Diese sind aber gut in der Installationsdokumentation beschrieben. Ebenso müssen noch die Zusatzfunktionen wie DCC, Razor und Pyzor separat installiert werden. Letztere drei dienen vor allem der Erkennung von Bulkmails. Das können auch normale Massenmails von Mailing-Listen sein.

Damit der Bayes-Filter aktiviert werden kann, muss dieser mit einem gewissen Anteil an Spam- und Ham- (erwünschten) Mails gefüttert werden. So kann die entsprechende Gewichtung vorgenommen werden.

Für die normalen Filterregeln mit den regulären Ausdrücken gibt es als Erweitungsmöglichkeit die sogenannten «Rules du jour» [9]. Da die normalen SpamAssassin-Filterregeln nicht alle Spam-Varianten erkennen, ist es möglich, mit diesem Script laufend vom Internet aktualisierte Filterlisten runterzuladen.

In Anwendung der Filterregeln wie auch der anderen Filter werden entsprechende Positiv- oder Negativpunkte vergeben. Je mehr Punkte ein Mail erhält, desto eher handelt es sich dabei um ein Spam-Mail.

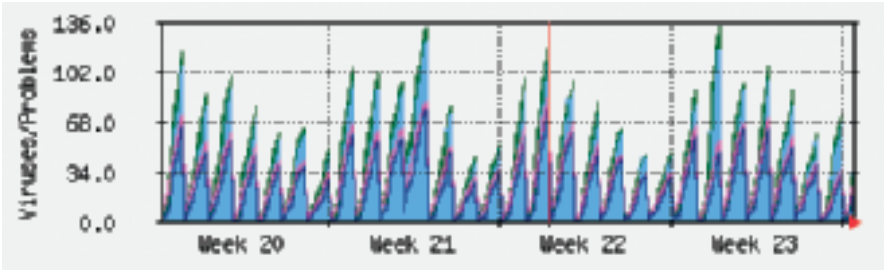

Abbildung 1. *Monatsstatistik des Wurmaufkommens.*

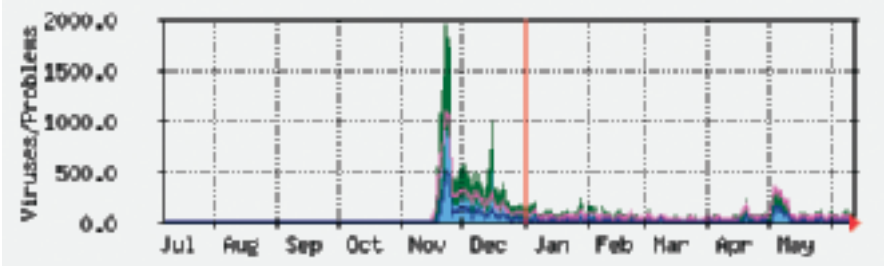

Abbildung 2. *Jahresstatistik des Wurmaufkommens. Gut sichtbar im November die Reduktion durch das Greylisting. Die Statistik reicht nicht weiter zurück, da zu diesem Zeitpunkt ein Server-Wechsel stattfand.*

Zu den Filterregeln mit den regulären Ausdrücken kann man auch diverse DNS-basierte Blacklists verwenden, die ebenfalls entsprechend gewichtet werden können.

Falls für gewisse Filterregeln zu viele Punkte vergeben werden, kann man diese mit einem eigenen Config-File anpassen, so dass nur wenige oder keine Punkte vergeben werden.

Konfiguration der Umgebung

Ein wesentlicher Punkt folgt nun in der Konfiguration der Umgebung, vor allem auch mit Mailscanner. Die Informatik des USZ verfolgt schon lange die Policy, dass ausführbare Inhalte (.exe, .bat, .com, .vbs, .pif, .lnk usw.) von Mails grundsätzlich nicht akzeptiert werden. Dies geschah schon länger auf den Exchange-Servern und wird neu auch auf dem externen Gateway so gehandhabt. Die Vergangenheit hat mehrfach gezeigt, dass eine gewisse Zeit nötig ist, bis die Antivirensoftware-Hersteller ihre Signaturmuster auf den aktuellen Stand gebracht haben und diese auch zur Verfügung stellen.

Bei grösseren Epidemien kann dies schon dazu führen, dass die Würmer ungehindert auf die Mailboxen der Benutzer gelangen. Und es hat sich auch gezeigt, dass diese Mails häufig von den Benutzern geöffnet werden.

Leider werden Würmer auch als .zip verschickt. Wenn man Dateien mit dieser Endung verbieten will, braucht es auch eine entsprechende Benutzerschulung, damit solche verpackten Dateien verschickt werden können. Mailscanner bietet auch die Möglichkeit, Passwort-geschützte .zip-Dateien nicht durchzulassen.

Neben den normalen Tests auf die Dateiendungen bietet Mailscanner auch die Möglichkeit, Dateien, die nicht dem normalen Namensmuster entsprechen, zu entfernen. Dies können zum Beispiel Dateien mit mehreren Endungen oder solche mit mehreren Leerschlägen (Whitespaces) sein.

Bei den Wurmmails ist es möglich, dass diese an die Benutzer weitergeleitet werden oder dass diese Mails gar nie beim Empfängerpostfach, sondern direkt auf dem Server in der Quarantäne landen. Es empfiehlt sich

Abbildung 3. *Übersicht über die Statistiken von Mailscanner-mrtg.*

aber auf jeden Fall, dass man als Administrator eine Nachricht erhält, wenn ein verseuchtes Mail eingetroffen ist. Es lässt sich so auch eruieren, wer der eigentliche Urheber der Mail ist. Häufig haben die Benutzer das Problem, dass sie das Gefühl haben, dass jemand ihnen ein Mail geschickt hat, da sie die Absenderadresse kennen. Es ist aber in den meisten Fällen so, dass die Würmer ihre Absenderadresse aus dem Adressbuch des verseuchten PC entnehmen und sich so als verschiedene Absender ausgeben.

Bei uns werden die Mails an die Benutzer weitergeschickt, aber der Wurm durch eine Textnachricht ersetzt. Bei Makroviren (Word, Excel), bei denen sich der Dateianhang säubern lässt, werden die Anhänge an die Benutzer weitergeschickt.

Bei Spam wird die Möglichkeit geboten, Spam-Mails als Dateianhang weiterzuschicken. Hier kann man eine Unterscheidung machen zwischen Mails, die eine bestimmte Punktzahl erreichen. In der Konfiguration des USZ werden Mails über 10 Punkte als Dateianhang weitergeschickt. Zwischen 5 und 10 Punkten wird ein Mail als Spam markiert. Die Wahrscheinlichkeit, dass hier Mails fälschlicherweise als Spam deklariert werden, ist noch grösser, als wenn diese eine hohe Punktzahl erreichen.

Zusätzlich bietet Mailscanner auch die Möglichkeit, Formulare, JavaScript, Phishing, IFrame und andere aktive Inhalte in HTML-Mails zu erkennen und je nach Konfiguration zu entfernen oder zu deaktivieren. HTML-Mails können auch gleich in Textnachrichten umgewandelt werden.

Aus Sicherheitsgründen empfiehlt es sich, alle aktiven Möglichkeiten in HTML-Mails zu deaktivieren. Über diese Wege wird verhindert, dass unkontrolliert Scripts auf dem PC ausgeführt werden, die zu einem Download von Trojaner führen können.

Die Meldung, die an die Benutzer geschickt wird, lässt sich nach den eigenen Bedürfnissen konfigurieren. So bestehen verschiedene Vorlagen für die verschiedenen Meldungen, die von Mailscanner erzeugt werden.

Monitoring der Umgebung

Wie schon erwähnt, existieren zum Monitoring der Umgebung verschiede Werkzeuge.

Um eine einfache Überwachung über die Auslastung der Hardware zu haben, hat sich HotSaNIC [4] bewährt. So sieht man auf einen Blick die wichtigsten Parameter wie CPU-Auslastung, Load des Servers, Anzahl der Prozesse, Auslastung der Netzwerkkarte, Auslastung der Harddisks und diverse andere Werte. So lässt sich im Dauerbetrieb abschätzen, ob die Hardware die Last, die für alle Funktionen nötig ist, überhaupt zu verarbeiten mag. Wichtig ist hier vor allem, dass genügend Arbeitsspeicher (Ram) vorhanden ist, da viele Funktionen für das Mailscanning speicherintensiv sind.

Für die Überwachung des Mail-Verkehrs wird am USZ Mailscanner-mrtg [5] eingesetzt. Damit sieht man auf einen Blick, wie sich die Maillast auf dem Server verhält. So werden auch Statistiken über die aktuell gefundenen Würmer, Anzahl Spam-Mails und natürlich auch die Menge der Mails inklusive des transportierten Datenvolumens angezeigt. Damit alle Funktionen genutzt werden können, muss das Logging in Mailscanner so konfiguriert werden, dass alle Informationen ins Logfile geschrieben werden. Wie die Statistiken bei Mailscanner-mrtg ausschauen, ist in den Bildern dargestellt.

Erfahrungen im Betrieb

Aus Sicht des Server-Betriebs haben sich die getroffenen Massnahmen vollends bewährt. So konnte der Spam- und Wurmanteil massiv reduziert werden und die Erkennungsrate von Spam ist hoch. Als Beispiel sind Statistiken zu dem Spam- und Virenaufkommen dargestellt. Es muss jedoch berücksichtigt werden, dass bei der Kurve zu Spam sehr viel am Mailserver blockiert wird (dunkelblaue Kurve) und nur ein sehr kleiner Anteil effektiv noch durchkommt. Davon wiederum ist ein gewisser Teil Würmer, da diese aufgrund bestimmter Merkmale auch als Spam deklariert werden.

Dies ist auch der Grund, dass in der Jahresstatistik die Kurve im Januar abfällt, da sich da einer der aktiven Würmer deaktiviert hat. Das Gesamtvolumen an Mail beträgt etwa 19 000 Mails, die täglich durch den Server gehen. Aus Resourcen-Gründen wurde das Scanning von ausgehenden Mails für den Spam- und Wurmfilter momentan nicht aktiviert. Wenn sich aber zeigen sollte, dass Würmer sich über den vorgesehenen Kanal verschicken sollten, ist das Scanning sicher zu aktivieren.

Von Benutzerseite gab es zur Spam-Filterung bislang sehr wenige negative Reaktionen. Für gewisse Mailing-Listen mussten Anpassungen vorgenommen werden, da diese teilweise Mails verschicken, die die gleichen Muster wie Spam-Mails aufweisen. Häufig handelt es sich dabei um HTML-Mails.

Mit dem Greylisting konnte der Anteil an Spam- und Wurmmails auch nochmals massiv reduziert werden. Greylisting kann auch gewisse Probleme bieten, wenn der Mailserver, der ein Mail schicken will, gewisse Standards nicht einhält oder kennt. Die Greylisting-Funktion schickt dem anderen Mailserver einen temporären Fehler. Ab diesem Zeitpunkt läuft ein Counter mit einem definierten Zeitwert (z. B. 300 Sek.). Wenn dieser Counter abgelaufen ist, nimmt der Server die Mail an, wenn diese wiederum von der gleichen IP-Adresse, Absenderadresse und Empfängeradresse stammen. Grundsätzlich können auch Würmer oder Spammer einen weiteren Zustellversuch mit diesen drei oben genannten Kriterien unternehmen und die Mail wird dann auch angenommen.

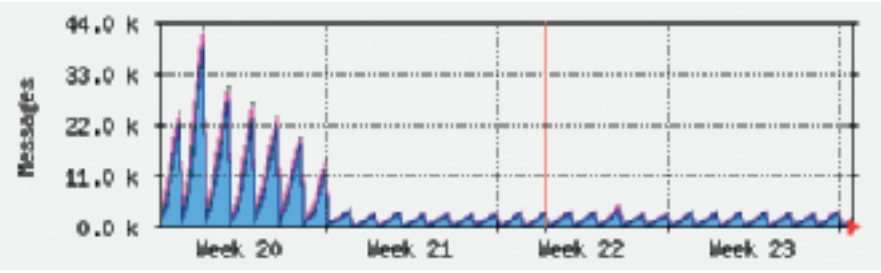

Abbildung 4. *Monatsstatistik über das Spam-Aufkommen. Die Skala unter Message bezieht sich auf die Anzahl Mails, die blockiert wurden (dunkelblaue Linie) oder das Total (Pink).*

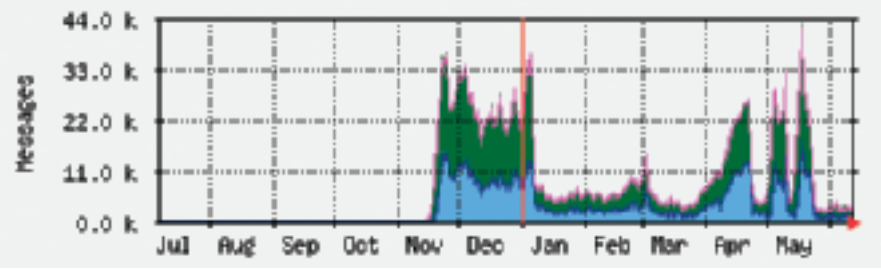

Abbildung 5. *Jahresstatistik über das Spam-Aufkommen. Der Rückgang im Januar ist auf eine Selbstabschaltung eines Wurms zurückzuführen.*

Allgemeine Überlegungen zu Spam- und Wurmfilterung

Auch wenn die Spam- und Wurmfilterung auf dem gleichen System geschehen, sind es doch zwei verschiedene Mechanismen, die dahinter stehen.

Bei einem Wurm- oder Virenmail ist aufgrund von Mustern in der Regel klar erkennbar, ob das Mail verseucht ist oder sogar nur einen Wurm enthält. Es ist eine Frage der Policy oder der Benutzerinformation, ob man solche Mails an die Benutzer weiterleiten will oder nicht. Grundsätzlich sollte den Benutzern aber auch bewusst sein, dass es solche Mails gibt und sie lokal auf ihrem Client die Möglichkeit haben, diese Mails zu löschen bzw. entsprechende Filterregeln einzurichten. Erfahrungsgemäss gibt es aber einige Benutzer, die sich gestört fühlen, wenn sie Würmer oder Unzustellbarmeldungen (Bounces) von solchen Würmern erhalten. Gerade letzteres lässt sich leider nicht vermeiden, da der Absender ja gefälscht werden kann und dieser nicht verifiziert wird.

Adressfälschung wird häufig auch bei Spam-Mails angewendet, um die eigentliche Absenderadresse zu verstecken.

Bei Spam-Mails ist es schwieriger festzulegen, ob diese auf dem Gateway gelöscht oder an die Benutzer weitergeleitet werden. Wird dies gemacht, so sollte dies auch gegenüber den Benutzern so kommuniziert werden. Zusätzlich sollten nur Mails gelöscht werden oder in die Quarantäne gehen, wenn diese eine bestimmte Punktzahl übersteigen. Ansonsten ist die Gefahr zu gross, dass erwünschte Mails den Empfänger nicht erreichen. Neben der Greylisting-Funktion gibt es auch noch die Möglichkeit, DNS-basierte Blacklists zu verwenden, um Mails direkt auf dem MTA zu blockieren, so dass diese nicht zugestellt werden. Diese sind mit einer gewissen Vorsicht zu verwenden, da es sonst dazu führt, dass man eine entsprechende Whitelist von erwünschten Mailservern führen muss. Zusätzlich werden diese auch von SpamAssassin zur Punktebeurteilung verwendet.

Je nach dem empfiehlt es sich auch, gewisse dynamische Netze von Providern, die immer wieder Probleme verursachen, direkt zu blockieren. Es ist aber zu beachten, dass sich teilweise hinter ADSL- oder Cablemodem-Anschlüssen fixe IP-Adressen verstecken und immer mehr Firmen dahinter eine Mail-Umgebung betreiben.

Für viele Funktionen, die auf dem Mailscanner ausgeführt werden, lassen sich benutzerdefinierte Regeln erstellen. So ist es auch möglich, Benutzer, die ihre Spam-Mails selber aussortieren, diese ohne Scanning weiterzuleiten. Bei anderen Funktionen ist es nicht in jedem Fall sinnvoll, da sonst die Sicherheit gefährdet werden kann. Es gibt auch Benutzer, die am liebsten keine Spam-Mails haben. Es bedarf eines gewissen Aufklärungsbedarfs, dass es je nach dem in ihrer Verantwortung liegt, mit der Mail-Adresse vorsichtig umzugehen. Eine Mail-Adresse, die im Internet auf Webseiten bekannt wird, ist vor Spam-Attacken eher gefährdet. So sollten diese auch nicht mehr einfach auf Firmenwebseiten präsentiert werden oder nur funktionelle Adressen verwendet werden. Auch empfiehlt es sich, nicht dem Wunsch nachzugeben und alle Mails, die als Spam erkannt werden, zu löschen. Früher oder später vermisst die gleiche Person ein wichtiges Mail.

Vergleich zu kommerziellen Produkten

Die aufgezeigte Lösung ist eine von mehreren Varianten. Es existieren einige kommerzielle Lösungen. Bei einer gewissen Menge von Benutzern kommen die Lizenzkosten bei gewissen Produkten in Bereiche, für die man eine Person anstellen kann, die sich fast nur um die Mail-Systeme bzw. um die Spam-Filter kümmert. Es gibt auch Lösungen, die an die Benutzer nur eine Meldung schicken, dass ein Spam-Mail oder ein Dateianhang in der Quarantäne liegt und dieses Mail abgerufen werden kann. Bislang kam es aber selten vor, dass dies effektiv ein Wunsch war bzw. in den seltenen Fällen kann der Dateianhang manuell nachgeliefert werden. Oftmals ist auch ein Hinweis an die Benutzer nötig, dass sie das nächste Mal die Datei richtig schicken.

Andere Spam-Filter-Lösungen basieren auf eigenständiger Hardware, sogenannten Appliances, die teilweise wiederum auf Open-Source-Lösungen, teilweise auch mit SpamAssassin basieren und eine fertig konfigurierbare Oberfläche bieten. Diese bieten aber nicht unbedingt die Flexibilität eines eigenständigen Mail-Servers. Für kleinere Umgebungen kann dies aber sicher eine Lösung darstellen.

Ebenso gibt es auch andere Open-Source-Lösungen, die Mails bereits beim Einliefern kontrollieren. Es ist da aber teilweise schwieriger, separate Filterlisten für spezielle Benutzerbedürfnisse zu führen.

Glossar

MTA = Message Transfer Agent: Mailgateway, das eine Mail an einen weiteren MTA weiterreicht oder lokal in die Postfächer überreicht.

Weiterführende Links

1 ttp://www.mailscanner.info
2 http://www.postfix.org
3 http://spamassassin.apache.org/
4 http://hotsanic.sourceforge.net/
5 http://mailscannermrtg.sourceforge.net/
6 http://sbserv.stahl.bau.tu-bs.de/~hildeb/postfix/
7 http://isg.ee.ethz.ch/tools/postgrey/
8 http://www.clamav.net/
9 http://www.exit0.us/index.php?pagename=RulesDuJour