K.G. Saur Verlag, München, 2008

M. Diehn, H. Reiser, B. Schmidt und M. Storz

Effiziente und effektive Spam-Abwehr: Konzepte und Verfahren

Max Diehn ist seit Ende 2004 wissenschaftlicher Mitarbeiter in der Gruppe Directories und E-Mail der Abteilung Benutzernahe Dienste und Systeme des Leibniz-Rechenzentrums (LRZ) der Bayerischen Akademie der Wissenschaften. Er beschäftigt sich dort u.a. mit den Bereichen Datenbankadministration, Aufbau einer MS Exchange Umgebung nebst delegierter Administration für getrennte, teils kooperierende Mandanten, Anbindung von Directories und Administration von Mailrelays. Im Rahmen der Anti-Spam Strategie des LRZ baute er das Greylisting-System mit Hochverfügbarkeit, Master-Master Replikation der Datenbanken, Glue Code zu den SMTP-Servern, Monitoring etc auf. Im Rahmen des DFG-geförderten Projekts IntegraTUM der TU München arbeitet er u.a. an der Re-Zentralisierung der gewachsenen, heterogenen und fragmentierten E-Mail Infrastruktur und Serverlandschaft. Er hat an der Universität Regensburg BWL mit Schwerpunkt Wirtschaftsinformatik studiert. Seine IT-Interessen liegen u.a. in den Bereichen Security, Operations Research und Software-Entwicklung.

Dr. *Helmut Reiser* ist Leiter der Gruppe Netzplanung am LRZ und stellvertretender Abteilungsleiter der Abteilung Kommunikationsnetze. Er ist für die Planung, Vernetzungskonzepte und Fragen der Netzsicherheit im Münchner Wissenschaftsnetz (MWN) zuständig. In seiner Gruppe sind auch Forschungsprojekte im Rahmen von D-Grid und Geant2 angesiedelt, die sich u.a. mit Fragen des Monitoring in Grids und paneuropäischen Forschungsnetzen sowie dem Betrieb und dem Management großer verteilter Infrastrukturen beschäftigen. Er hat an der Technischen Universität München Informatik studiert (Diplom 1997) und an der Ludwig-Maximilians Universität (LMU) 2001 über Sicherheit in Managementsystemen promoviert. Von 1997 bis 2005 war Dr. Reiser am Lehrstuhl Kommunikationssystem und Systemprogrammierung der LMU (MNM-TEAM) beschäftigt. Seine Forschungsinteressen liegen im Bereich Sicherheit insbesondere in föderierten Umgebungen, Grid Technologien und dem integrierten IT-Management Er ist Mitglied der GI und IEEE.

Bernhard Schmidt beschäftigt sich seit 2001 mit Planung und Betrieb von Netzen und war bis zum Jahr 2004 bei mehreren nationalen Providern, teilweise in verantwortlicher Position, tätig. Seit seinem Studienbeginn gehört er der Abteilung Kommunikationsnetze des LRZ an und war an der Entwicklung sowie dem Auf- und Ausbau vieler Dienste, beteiligt, unter anderem dem NAT-o-MAT, dem DNS und den neuen Mailrelays. Seine besondere Hingabe gilt der Verbreitung von IPv6 im globalen Umfeld, unter anderem in diesem Zusammenhang ist er aktives Mitglied bei der europäischen Dachorganisation RIPE und bei verschiedenen anderen Interessensverbänden und Communities. Seine Arbeitsschwerpunkte umfassen auch weiterhin auf freiberuflicher Ebene das volle Dienstspektrum von Internet-Service-Providern.

Michael Storz studierte an der Technischen Universität München Informatik. Er ist seit 1982 am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften angestellt, zuerst als studentischer Operateur, seit 1986 als wissenschaftlicher Angestellter im Bereich Kommunikationsnetze. 1987 sollte er nur für kurze Zeit einen Kollegen bei der Betreuung des E-Mail-Anschlusses an das EARN/Bitnet unterstützen. Wenige Monate später war es seine Hauptbeschäftigung und heute leitet er das E-Mail-Team, das inklusive der Projektstellen aus fünf wissenschaftlichen Mitarbeitern besteht. Sein Arbeitsschwerpunkt innerhalb des Teams ist der Betrieb der Mailrelays und die Konzeption der Anti-Spam-Maßnahmen.

1 ZUSAMMENFASSUNG

Die Flut an unerwünschten Werbemails (Spam) hat in den letzten Jahren dramatisch zugenommen. Spam ist nicht nur für den Endnutzer, der den Müll in seiner Mailbox vorfindet, ärgerlich, sondern verursacht auch einen erheblichen finanziellen Aufwand und Schaden durch zusätzlich benötigte Ressourcen zur Verarbeitung oder Bekämpfung von Spam sowie Vergeudung von Arbeitszeit. Im Leibniz-Rechenzentrum (LRZ), das eine große E-Mail-Infrastruktur für sehr viele Kunden betreibt, hat sich das Spamaufkommen im Jahr 2007 verdreifacht, während die Anzahl der regulären E-Mails schon seit längerem relativ konstant bleibt. Die Spam-Rate ist dadurch auf 98% gestiegen.

In diesem Artikel wird das sehr effektive und effiziente Anti-Spam-Konzept des LRZs mit seinen verschiedenen Maßnahmen präsentiert. Die Grundidee dabei ist, die *Übertragung* von unerwünschten E-Mails mit Hilfe von *Ressourcen-schonenden* und *rein formalen, nicht den Inhalt der E-Mails inspizierenden* Verfahren so weit wie möglich zu verhindern. Das bedeutet, die

10.1515/piko.2008.0031

infizierten Rechner, die E-Mails aus dem Münchner Wissenschaftsnetz *ins Internet* schicken wollen, bereits auf der IP-Ebene zu blockieren und die *aus dem Internet* ankommenden E-Mails erst gar nicht anzunehmen.

Die wichtigsten dazu eingesetzten Verfahren sind:

- Statistische Analyse der Anzahl an abgehenden SMTP-Verbindung eines Rechners
- Ablehnung von Mailservern mit dynamisch zugewiesenen IP-Adressen
- Ablehnung von Mailservern mit inkonsistenter DNS-Konfiguration
- Frühzeitige Verifizierung von Empfangsmailadressen

Diese Verfahren sind einfach zu implementieren und dabei so erfolgreich, dass in beiden Richtungen, trotz der extremen Spam-Rate, nur noch wenige Spammails übertragen werden. Gleichzeitig ist der Ressourcen-Einsatz relativ gering, sodass mit einer kostengünstigen Infrastruktur gearbeitet werden kann.

2 ANWENDUNGSFELD: DAS LEIBNIZ-RECHENZENTRUM

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften ist das Hochschulrechenzentrum für die Ludwig-Maximilians Universität München (LMU), die Technische Universität München (TUM) und die Bayerischen Akademie der Wissenschaften [1]. Es ist Zentrum für technisch-wissenschaftliches Hochleistungsrechnen (Nationales Supercomputing-Zentrum) für alle deutschen Hochschulen, es betreibt umfangreiche Platten- und automatisierte Magnetband-Speicher zur überregionalen Sicherung und Archivierung großer Datenmengen. Mit dem Münchner Wissenschaftsnetz (MWN) wird eine leistungsfähige Kommunikationsinfrastruktur auch für zahlreiche weitere Hochschulen und Wissenschaftsinstitutionen im Großraum München bereitgestellt [2]. Daneben bietet das LRZ seinen Kunden eine Vielzahl von Diensten an, etwa bayernweiter Einkauf von Lizenzen, Beratung, Kurse sowie Spezial-Hardware (z.B. im Bereich Visualisierung und Multimedia) [3].

Ein zentraler Dienst ist E-Mail [4], den das LRZ für die Studenten und Mitarbeiter der am MWN angeschlossenen wissenschaftlichen Einrichtungen erbringt. Es betreibt dazu Mailrelays zwischen dem Internet und dem MWN zur zentralen Abwehr von Spam und Viren. Diese Relays leiten die entgegengenommen E-Mails weiter – entweder zu einem der mehrere hundert lokalen Mailserver, z.B. eines Lehrstuhls, oder zu einem der zentral vom LRZ betriebenen Message Stores (Mailbox-Server).

Das LRZ bietet den Einrichtungen an, ihren Maildienst am LRZ zu „hosten“. Dazu wird eine *virtuelle Maildomain* für die betreffende Einrichtung (z.B. *jura.uni-muenchen.de*) angelegt und Angehörige dieser Einrichtung erhalten entsprechende Mailadressen. Ende 2007 waren am LRZ mehr als 220 solcher virtuellen Maildomains eingerichtet und knapp 100.000 Nutzer hatten eine Mailbox auf einem der zentralen Message Stores.

Von den LRZ-Relays wurden im Februar und März 2008 im Monatsdurchschnitt täglich gut 6 Millionen, Mitte 2007 an Spitzentagen sogar bis zu 20 Millionen E-Mails verarbeitet [5].

Im folgenden Kapitel werden verschiedene Spam-Arten und deren Hauptquellen eingeführt. Kapitel 4 beschreibt die am LRZ realisierten Spam-Abwehrmaßnahmen für die beiden Richtungen MWN → Internet und Internet → MWN. Kapitel 5 stellt die Betriebserfahrungen dar.

3 SPAM: DEFINITION UND HERKUNFT

Wenn im Folgenden der Begriff Spam bzw. Spammail verwendet wird, so bezieht er sich immer auf das Kommunikationsmedium *E-Mail* – Spam ist bei allen Medien möglich, z.B. News, SMS, VOIP – und auf alle E-Mails, die in der Regel *massenweise* verschickt und vom Empfänger *unerwünscht* sind (unsolicited bulk email = UBE). Einbezogen darin sind auch indirekt entstandene Spammails, die als *Backscatter-Spam* oder *kollateraler Spam* bezeichnet werden. Das Gegenteil von Spam, die „guten“ E-Mails, werden mit dem Begriff *Ham* bzw. *Hammails* bezeichnet.

Die Einteilung der E-Mails in Ham und Spam ist sehr unscharf, da die Eigenschaft „unerwünscht“ oft nur subjektiv entschieden werden kann. Eine Bewertung aller Maßnahmen zur Reduktion der negativen Auswirkungen von Spammails kann daher im Endeffekt nur aus Sicht des Empfängers der E-Mails geschehen. Aus seiner Sicht ist ein „false positive“ eine Hammail, die fälschlicherweise als Spam gebrandmarkt wurde, und ein „false negative“ eine Spammail, die nicht als solche erkannt wurde.

Um zu geeigneten Maßnahmen im Kampf gegen die Spamflut zu kommen, muss man sich zuerst darüber im Klaren werden, aus welchen Quellen die Spammails stammen.

3.1 Spam durch Botnetze

Bereits 2006 wurden nach Angaben von Ironport [6], einem Anbieter von Anti-Spam-Lösungen, mehr als 80% aller Spammails von Botnetzen [7] verschickt. Heutzutage dürfte der Prozentsatz noch höher liegen. Nach Schätzungen von SecureWorks [8], einem Security Services Provider, umfassen die zehn größten Botnetze nur 1.000.000 Bots (= infizierte Rechner) (Stand März 2008). Sie sind aber in der Lage bis zu 136 Milliarden Spammails pro Tag zu verschicken. Da die Anzahl der pro Bot und Tag verschickten Spammails um den Faktor 10 schwankt, von 29.000 beim Botnetz SpamThru bis zu 286.000 bei Ozdok, geht SecureWorks davon aus, dass der Höhepunkt an verschickten Spammails noch lange nicht erreicht ist, insbesondere da Ozdok mit 35.000 Bots relativ klein gegenüber dem größten Botnetz Srizbi mit 315.000 Bots ist. Die Analysen von Marschall [9], einem Anbieter von Security Lösungen im Bereich E-Mail, zeigen prozentual eine ähnliche Größenordnung bei der Anzahl der verschickten Spammails, wobei aber auch ersichtlich ist, dass sich die Zahlen von Monat zu Monat stark ändern können, also jeweils nur eine Momentaufnahme darstellen.

Am Anfang, beginnend mit dem Botnetz, das im Jahre 2003 mit Hilfe der Wurmfamilie Sobig aufgebaut wurde, waren die Botnetze Proxy-basiert, d.h. auf jedem Bot wurde durch die Schadsoftware ein Proxy installiert. Die Botnetz-Betreiber hatten dadurch immer genügend Proxys zur Verfügung, mussten aber weiterhin die Ressourcen/Rechner zur Verfügung stellen, die die eigentliche Arbeit des Spammail-Versendens übernahmen. Die verwendeten Engines, die das Mailprotokoll SMTP (Simple Mail Transfer Protocol) [10] implementieren, waren darauf optimiert, große Mengen an E-Mails in möglichst kurzer Zeit zu generieren und zu verschicken. Daher wurden aus Performance-

gründen die Details der Protokolllogik, die nicht diesem Zwecke dienten, nicht implementiert.

Mit dem Aufkommen der Template-basierten Botnetze – nach SecureWorks sind die momentanen großen Botnetze alle Template-basiert – änderte sich dies. Statt einem Proxy wird jetzt auf jedem Bot eine SMTP-Engine installiert. Der Bot wird nur noch mit einem Spam-Template und einer Liste von Mailadressen versorgt. Danach übernimmt er die Zustellung der E-Mails in eigener Regie, ohne irgendwelche zentralen Ressourcen zu benötigen. Dadurch haben die Botnetzbetreiber die Möglichkeit gewonnen, die Bots beinahe wie reguläre Mailserver (Message Transfer Agents, MTA) zu betreiben.

3.2 Spam von Wegwerfaccouts

Eine zweite, erst in den letzten Wochen wieder verstärkt genutzte Quelle von Spammails, sind „Wegwerfaccounts“ bei Freemailern. Lange Zeit konnten die Freemailer das massenweise automatische Anlegen von Accounts durch den Einsatz der CAPTCHA-Techniken (Completely Automated Public Turing test to tell Computers and Humans Apart) verhindern. Inzwischen ist es den Spammern aber unter Einsatz ihrer Botnetze gelungen, diese Techniken auszuhebeln [11].

3.3 Weitergeleiteter Spam

Nicht unerheblich kann, insbesondere im wissenschaftlichen Umfeld, der Anteil an Spammails werden, der durch Weiterleitungen der E-Mails von fremden MTAs an Adressen der eigenen Domain entstehen. Ist die Spamabwehr des fremden MTA nur schwach ausgeprägt, so können dadurch enorme Mengen an Spammails ins eigene System gelangen. Im LRZ ist ein Fall aufgetreten, bei dem 8,75% aller angenommenen E-Mails Spammails für einen einzigen Benutzer waren. Solche extremen Fälle kommen zustande, wenn jemand einen Mailserver bei einem Provider (ISP) hosten lässt, der ohne eine Spamabwehrmaßnahme betrieben wird, und E-Mails für jede beliebige Adresse der Empfangsdomain entgegen.

3.4 Backscatter-Spam

Backscatter-Spam, d.h. indirekter Spam durch „Rückstreuung“, entsteht für eine Domain, wenn ein Spammer als Absendemailadressen für seine Spammails Mailadressen aus der Domain verwendet, die dadurch Ziel des Backscatter-Spam wird. Wenn der zuständige Empfangs-MTA die Spammail annimmt und versucht sie zuzustellen, kann als Reaktion eine neue E-Mail entstehen, die dann an die Absendemailadresse geschickt wird. Diese neu erzeugte E-Mail wird als Backscatter-Spammail bezeichnet.

Es gibt verschiedene Gründe für das Entstehen einer neuen E-Mail. Zum größten Teil handelt es sich um Fehlermeldungen (DSN = Delivery Service Notification) wegen nicht existierendem Empfänger. Weitere Arten sind automatische Antworten wie z.B. Abwesenheitsmeldungen, Anti-Spam-Systeme, die eine Nachricht über die Blockade der Spammail verschicken, oder Anti-Spam-Systeme auf Basis von Challenge-Response [12], die die „Kosten“ für die Spamabwehr auf Unschuldige abwälzen.

Verwendet der Spammer real existierende Absenderadressen, so erreichen die Backscatter-Spammails auch die Nutzer-Mailboxen, andernfalls werden nur die Mailserver der Backscatter-Domain belastet.

4 ABWEHRMAßNAHMEN

Bei der Auswahl geeigneter Anti-Spam-Maßnahmen muss neben der Herkunft auch der Weg der Spammails von der Mailquelle (Mail User Agent, MUA) über das aus meist mehreren MTAs bestehende Message Transport System (MTS) bis hin zur Mailsenke (Message Store, MS) betrachtet werden. An jeder Stelle dieses Weges sind Anti-Spam-Maßnahmen möglich und sollten auch durchgeführt werden. Jeder, der einen Rechner mit Zugang zum Internet betreibt, muss sich darüber im Klaren sein, dass er Teil der Spamproblematik sein kann. Er sollte daher alle notwendigen Maßnahmen durchführen, um nicht selbst zu einer Spamquelle zu werden.

4.1 E-Mails vom MWN ins Internet

Für das LRZ als Betreiber des MWN bedeutet dies, dafür zu sorgen, dass so wenig Spammails wie möglich das MWN verlassen. Nachdem das MWN – wie die meisten wissenschaftlichen Netze – ein sehr offenes Netz ist, ist die Gefahr sehr groß, dass sich einzelne Bots eines Botnetzes einnisten. Um neue Bots zu requirieren, präparieren Botnetz-Betreiber viele Web-Seiten so, dass bei einem Besuch der Seiten Sicherheitslücken im Browser ausgenutzt werden, um den Botnetz-Client auf dem Rechner zu installieren. Damit die Seiten nicht nur über Suchmaschinen gefunden werden, versenden die Botnetz-Betreiber Spammails, die die Empfänger mit Hilfe von „social engineering“ dazu verleiten sollen, die infizierenden Seiten zu besuchen. Man sieht also, dass gute Anti-Spam-Maßnahmen bereits an diesem Punkt helfen, den Teufelskreislauf etwas zu verlangsamen.

4.1.1 Die Update-Services des LRZ

Nachdem das LRZ nur einen kleinen Teil der Rechner im MWN administriert, muss sichergestellt werden, dass jeder einzelne Administrator eines Rechners so schnell wie möglich Sicherheitslücken schließt, Infektionen mit Schadsoftware beseitigt und die Signaturen der Anti-Viren-Software auf dem neusten Stand hält. Dafür bietet das LRZ zum einen mit einem eigenen *Windows Server Update Service (WSUS)* [13] die Möglichkeit, eine Reihe von Windows Betriebssystemen mit Updates direkt aus dem MWN zu versorgen, und zum anderen im Rahmen einer Landeslizenz für Bayern einen Virenscanner, der von allen Wissenschaftlern, Mitarbeitern von Universitäten und Forschungseinrichtungen sowie den Studenten kostenlos genutzt werden kann. Da vom LRZ ein lückenloser und flächendeckender Einsatz angestrebt wird, ist explizit auch die Nutzung für private Zwecke durch die Landeslizenz abgedeckt. Damit auch die Signaturen für die Schadsoftware immer auf dem aktuellen Stand sind, betreibt das LRZ einen eigenen automatischen Update Server für diesen Virenscanner [14].

4.1.2 Bot-Überwachung im MWN

Taucht ein Bot im MWN auf – es kann sich auch um einen privaten Mitarbeiter- oder Studentenrechner handeln, der über VPN Teil des MWN geworden ist – so müssen die Auswirkungen minimiert werden. Während bereits im Jahr 1998 der

SMTP-Port für E-Mails aus dem Internet ins MWN gesperrt wurde – E-Mails können nur noch über dedizierte Relays ins MWN gelangen – ist dies in der umgekehrten Richtung bisher nicht der Fall. Jeder Rechner des MWN kann daher theoretisch direkt E-Mails ins Internet senden.

Dennoch ist eine effektive Kontrolle möglich. Durch eine statistische Analyse der Anzahl an neu initiierten TCP/IP-Verbindungen werden auffällige Rechner – insbesondere auch Spamquellen – erkannt, ohne dass ein rechtlich fragwürdiger Einblick in den Inhalt der Datenströme erforderlich wird. Dazu werden zwei verschiedene Verfahren eingesetzt:

- Der komplette Verkehr aus den dedizierten Endnutzer-Netzen (Studentenwohnheime, WLAN/VPN-Nutzer, aber auch einige Lehrstuhlnetze) wird über ein selbstentwickeltes System namens NAT-o-MAT [15] geleitet. Dieses führt optional eine Adressumsetzung durch (NAT), überwacht die Verkehrsströme und greift regulierend ein (o-MAT). Hierzu werden Limitierungen, z.B. für die Anzahl der SMTP-Verbindungen pro Zeitabschnitt, festgesetzt. Im Fall des MWN sind generell zwei Verbindungen pro Minute für jede interne IP-Adresse zulässig. Überschreitungen werden automatisch blockiert und auf ein Punktekonto addiert. Überschreitet ein Rechner (IP-Adresse), z.B. aufgrund einer Bot-Infektion, diese Rate dauerhaft und schöpft damit sein Punktekonto aus, wird dieser Rechner vom Internet abgeschottet. Der Nutzer wird beim Aufruf einer Webseite auf eine interne Fehlerseite des NAT-o-MAT umgeleitet und dort über sein Problem aufgeklärt. Da dieser proaktive Ansatz eine Umleitung aller Verbindungen über Systeme erfordert, die wesentlich geringere Durchsatzraten als moderne hardwarebasierte Router haben, werden alle anderen IP-Netze über ein anderes Verfahren überwacht.
- Am Router zwischen dem MWN und dem Internet werden Statistikdaten über die Anzahl und Ziele aller SMTP-Verbindungen ins Internet generiert und protokolliert. Momentan geschieht dies über die Untersuchung des gespiegelten Datenverkehrs auf der 10GE Internet-Schnittstelle, soll aber in Zukunft durch die Analyse von Router-generierten Verbindungsdaten (Netflow-Records) abgelöst werden. Dies erfordert insbesondere keine Ausleitung des kompletten Datenverkehrs mehr, sondern exportiert die in den Routern gesammelten Informationen. Im Gegensatz zum NAT-o-MAT wird aufgrund dieser Informationen derzeit keine automatische Reaktion ausgelöst. Stattdessen findet eine manuelle Alarmierung, Untersuchung und Intervention statt. Ausnahmelisten dieses Tools verhindern die Alarmierung und eventuelle Sperrung von bekannten Mailservern und -quellen im MWN.

Kommt es zu einer Beschwerde, weil ein Bot aktiv und nicht erkannt bzw. nicht schnell genug gesperrt wurde, so wird unser Abuse-Response-Team aktiv, sperrt die IP-Adresse am Übergang ins Internet und informiert den zuständigen Netzverantwortlichen. Solche Fälle, in denen Spam-Quellen im MWN von extern gemeldet werden, kommen aber ausgesprochen selten vor.

Langfristig sollen auch alle vom MWN ins Internet abgehenden SMTP-Verbindungen komplett gesperrt werden und E-Mails nur noch über dedizierte Mailausgangsserver des LRZ verschickt werden können. Für die legitimen Nutzer externer Mailausgangsserver wurde bereits 1998 in RFC 2476 [17] der Port 587/tcp als zusätzlicher SMTP-Port definiert. Im Gegensatz zu Port 25 wird am Port 587 keine E-Mail – auch nicht an eigene Domains – ohne Authentifizierung des Senders angenommen, sodass dieser Dienst kein Loch in die Anti-Spam-Maßnahmen reißt. Diese Maßnahme wird bereits zunehmend von vielen Enduser-Providern durchgeführt und erfreut sich insbesondere in amerikanischen Kabelnetzen großer Beliebtheit.

In Fällen, in denen eine derart harte Vorgehensweise nur schwer durchzusetzen ist, sollte potentiellen Spam-Opfern wenigstens so viele Anhaltspunkte wie möglich gegeben werden, um mit Spammails aus dem eigenen Netz fertig zu werden. So gehören eine Markierung von Dialup-Zugängen mittels einschlägigen Reverse-DNS-Namen ebenso zum guten Ton wie das Listing eigener Adressbereiche in der PBL-Liste von Spamhaus [18]. Die PBL (Policy Block List) listet Adressbereiche, aus denen keine Mailquellen kommen sollten.Da in vielen Fällen die Zuordnung einer IP-Adresse zu einem ISP und damit einer Beschwerdestelle für Nicht-Eingeweihte schwierig ist, sollte diese Information auch explizit in der Datenbank der europäischen Vergabestelle für Internet-Ressourcen (RIPE) hinterlegt werden.

4.2 E-Mails vom Internet zum MWN

Die Spam-Abwehr für die Kunden des LRZ befasst sich mit E-Mails, die aus dem Internet ins MWN übermittelt werden. Neben den Relays des LRZ gibt es noch eine Reihe weiterer Relays, die von einzelnen Fakultäten wie Informatik oder Medizin für ihre Nutzer betrieben werden. Alle anderen Mailserver im MWN routen ihre E-Mails über die Relays des LRZ, auf denen unsere zentralen Anti-Spam-Maßnahmen implementiert sind.

Die Anti-Spam-Maßnahmen der LRZ-Relays teilen sich in zwei Phasen auf (s. Abb. 1)

- Phase I: Entscheidung anhand verschiedener Kriterien, ob eine E-Mail angenommen oder zurückgewiesen wird
- Phase II: Nach der Annahme der E-Mail: inhaltliche Bewertung, Sortierung und Markierung von Ham und Spam.

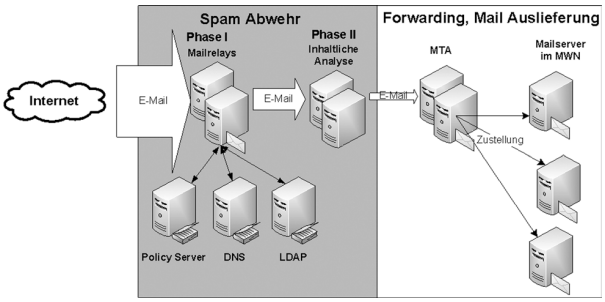

Abb. 1 Mail-Infrastruktur

In der Vergangenheit wurden vor allem die Maßnahmen der zweiten Phase eingesetzt. An den LRZ-Relays beträgt das Verhältnis von Ham- zu Spammails inzwischen 1 : 50, d.h. 98% aller E-Mails sind Spammails. Da die inhaltliche Bewertung sehr Ressourcen-intensiv ist, würde zur Bewertung aller Spammails eine enorme Anzahl an Rechnern benötigt. Selbst wenn diese Rechner zur Verfügung stehen würden, gäbe es noch einen zweiten Grund, warum die zweite Phase alleine nicht ausreicht. Da eine korrekte Bewertung nie mit hundertprozentiger Sicherheit erfolgen kann, muss der Empfänger zumindest den Graubereich an E-Mails auf false positives kontrollieren. Dies kostet zum einen erheblichen Arbeitsaufwand, zum anderen steigt mit

der Anzahl der zu kontrollierenden E-Mails die Wahrscheinlichkeit, einen false positive zu übersehen. Dies ist wesentlich schlimmer als fälschlicherweise eine E-Mail bereits bei der Annahme abzulehnen, da in diesem Fall der Sender eine Fehlermeldung bekommen sollte.

Daraus folgt, dass heutzutage der Schwerpunkt der Spamabwehr an den LRZ-Relays in Phase 1 liegen muss. So lehnten die LRZ-Relays im Monatsdurchschnitt im März 2008 täglich ca. 6 Millionen und damit ca. 99,5% aller Spammails ab. Im Folgenden wird daher nicht auf die Maßnahmen der Bewertung in Phase 2 eingegangen, sondern es werden die Highlights der Phase 1 vorgestellt.

Da aus Ressourcengründen auf eine inhaltliche Bewertung einer E-Mail in Phase 1 verzichtet werden muss, stehen als Kriterien für die Entscheidung über die Annahme einer E-Mail zum einen die Daten der verwendeten Protokolle als auch die Protokolllogik an sich zur Verfügung.

An Daten wären das im Wesentlichen

– die IP-Adresse des sendenden SMTP-Clients
– die Domain aus dem Protokollelement HELO bzw. EHLO
– die Mailadresse des Senders aus dem Envelope (nicht zu verwechseln mit der Adresse aus dem Header)
– die Mailadressen der einzelnen Empfänger aus dem Envelope

Auf den LRZ-Relays wird neben Greylisting (s. Abschnitt 4.2.3) eine Reihe von Überprüfungen der oben genannten Daten eingesetzt. Entscheidend für die Performance der Relays ist dabei die Reihenfolge der verschiedenen Überprüfungen. Diese sollten so angeordnet werden, dass „billige“ eher am Anfang und „teure“ am Ende kommen, wobei sich billig/teuer auf den Einsatz an Ressourcen und die durch die Überprüfung benötigte Zeit bezieht. So ist z.B. die Abfrage von Daten, die im Hauptspeicher liegen, sehr billig, während die Überprüfung einer Mailadresse über einen SMTP-Callout (s. Abschnitt 4.2.4) sehr teuer ist.

Die eingesetzten Maßnahmen und deren Reihenfolge sind im Ablaufdiagramm (vgl. Abb. 2) festgehalten. Näher erläutert werden die 4 Maßnahmen, die am meisten zur Abwehr beitragen (in der Abbildung grau hinterlegt):

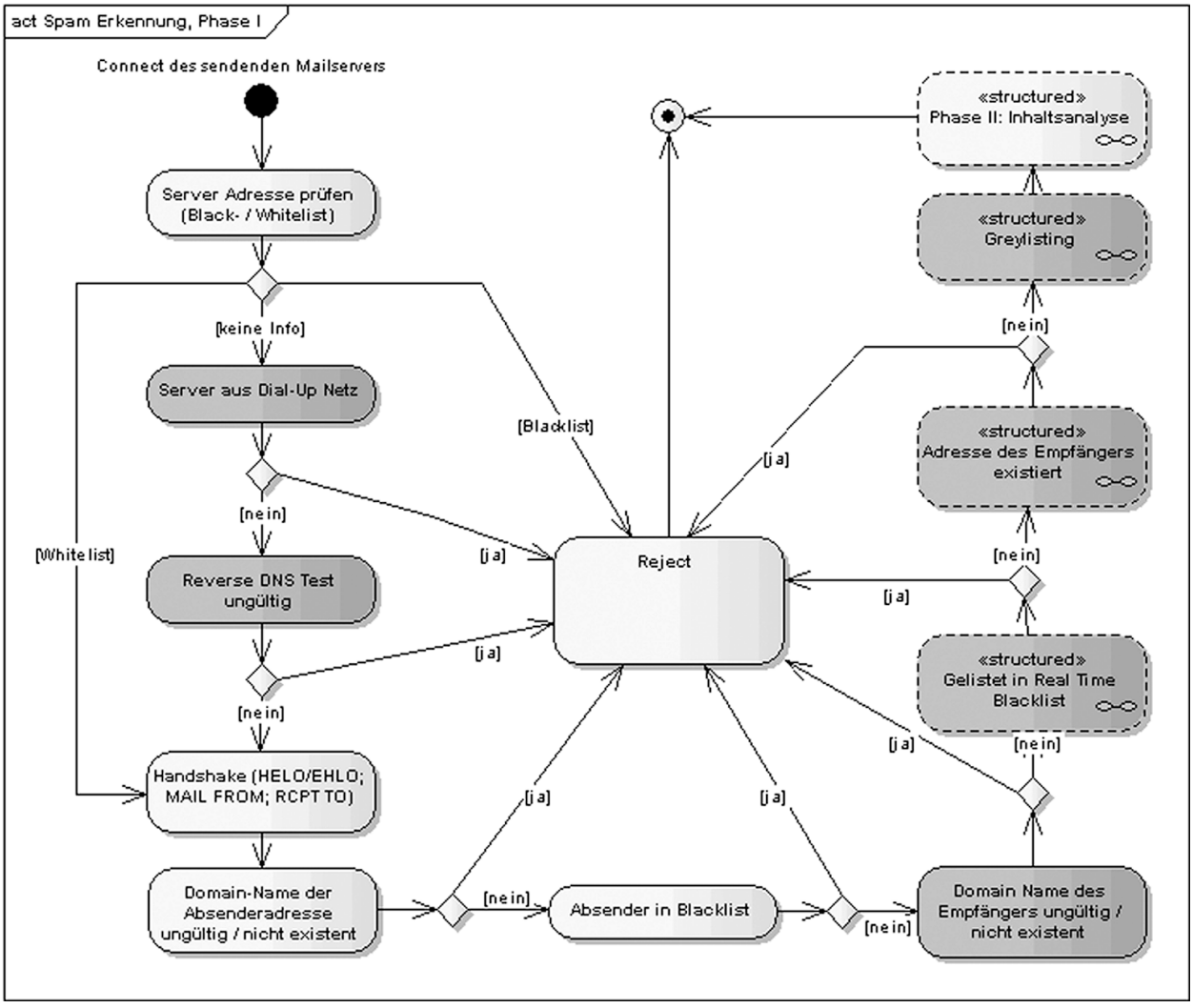

Abb. 2 Ablaufdiagramm der Anti-Spam-Maßnahmen (vereinfacht)

- Server aus Dialup-Netzen und Real Time Blacklisten
- Konsistenz-Check des Mappings zwischen der Caller-IP-Adresse und dem zugehörigen Domainnamen (Reverse DNS-Test)
- Greylisting
- Überprüfung der Empfangsadressen

Die Idee hinter den Maßnahmen der Phase 1 ist, dass im Wesentlichen formale Kriterien entscheiden, ob eine E-Mail angenommen oder abgewiesen wird, nicht aber, ob es sich bei dem Sender um einen Spamversender handelt. Diese formalen Kriterien sollten für den Sender einfach nachvollziehbar und möglichst auch einfach zu ändern sein. Da der größte Teil der Spammails von Botnetzen kommt, war das Ziel, Kriterien zu finden, mit denen ein Bot von einem regulären MTA unterschieden werden kann. Gelingt dies, so können Verbindungsversuche dieses Bots sofort abgewiesen werden, bevor eine E-Mail übertragen wird.

Unter einem regulären MTA wird ein korrekt implementierter, richtig konfigurierter und gut administrierter verstanden. Im Kampf gegen die Spammer kann und muss von jedem MTA-Betreiber erwartet werden, dass er seinen Anteil dazu leistet. Die richtige Konfiguration des MTAs und vor allem der zugehörigen Informationen im DNS, durch die die Gegenseite erkennen kann, dass dies ein solcher regulärer MTA sein soll, ist manchmal etwas aufwändiger, aber unbedingt notwendig. Insbesondere lokale Kommunikationsprobleme zwischen den Personen, die für die Administration des MTAs zuständig sind, und denen, die für die Administration des DNS verantwortlich sind, müssen lokal gelöst werden.

4.2.1 Server aus Dialup-Netzen

Die größte Verbreitung finden Bots auf privaten PCs von Home-Nutzer. Diese Gruppe scheint am wenigsten in der Lage zu sein, ihre Rechner adäquat zu administrieren, d.h. schnell mit Patches und aktuellem Virenscanner zu versehen. Zudem ist es die Gruppe, die am meisten im Internet surft und daher Gefahr läuft, auf eine präparierte Webseite zu stoßen und in der Folge ihren PC mit einem Bot zu infizieren. Auf der anderen Seite ist diese Gruppe oft breitbandig ans Internet angeschlossen und, bedingt durch die wachsende Anzahl an Flatrates, über längere Zeit online. Da außerdem die ISPs in der Regel keinerlei Missbrauchsüberwachung dieser PCs durchführen, ist es verständlich, warum man in dieser Gruppe die meisten Bots findet.

Die Rechner dieser Gruppe haben ein gemeinsames Merkmal, das sie identifizierbar macht. Bei jedem Verbindungsaufbau zum Internet bekommen sie dynamisch eine neue IP-Adresse zugewiesen. Im Gegenzug dazu haben reguläre MTAs in der Regel immer eine feste eindeutige IP-Adresse. Ist feststellbar, ob eine IP-Adresse dynamisch vergeben wird, so können diese – oft von einem Bot übernommenen Rechner – vom Mailverkehr ausgeschlossen werden.

Es stellt sich aber die Frage, ob durch diese Heuristik gleichzeitig auch reguläre MTAs in signifikantem Umfang ausgeschlossen werden. In der Tat gibt es eine kleine Gruppe an MTAs, deren Betreiber aus Kostengründen mit dynamischen statt statischen Adressen arbeitet. Nach sorgfältiger Abwägung sind wir aber zu der Ansicht gekommen, dass auch diese Gruppe ihren Anteil an den Kosten für die Bekämpfung von Spam tragen muss, indem sie entweder den MTA ihres Providers nutzt oder sich eine statische IP-Adresse zulegt.

Wie kann festgestellt werden, ob eine IP-Adresse dynamisch oder statisch vergeben wird? Am besten weiß natürlich der ISP darüber Bescheid, wie er einen bestimmten Adressbereich nutzt. Daher wäre es am einfachsten, wenn alle ISPs weltweit die Art der Nutzung dokumentieren und möglichst an einem zentralen Ort hinterlegen würden. Diesen Weg versucht das Spamhaus-Projekt [18] zu gehen. In ihrer DNS-basierten Blacklist (DNSBL) PBL sind diejenigen IP-Adressen markiert, die vom ISP bei Spamhaus als dynamisch gemeldet wurden, während der Rest der Adressen von Spamhaus zusammengestellt wurde. Diese DNSBL kann wie ein regulärer DNS-Server nach einer Adresse oder einem Host-Namen abgefragt werden. Falls der Anfragende eine spezielle Antwort erhält (z.B.: „127.0.0.11“), handelt es sich bei der Adresse um eine dynamisch zugewiesene. Leider ist nur ein kleiner Teil der ISPs bereit, daran mitzuarbeiten. Sofern die ISPs für die IP-Adressen PTR-Records im DNS angelegt haben, kann teilweise aus der Namensgebung die Verwendung entnommen werden. Zum Teil dokumentieren die ISPs die Verwendung der Netze in den jeweiligen whois-Einträgen im Netznamen oder in einem Kommentarfeld. Ansonsten bleibt nur noch eine statistische Auswertung, um eine Liste mit den dynamischen Adressen zu erstellen.

An den LRZ-Relays wird eine lokale Kopie der Spamhaus PBL eingesetzt. Da aber auch die PBL nur einen Teil der weltweiten dynamischen IP-Netze kennt, verwenden wir daneben auch 25 Regeln, die anhand regulärer Ausdrücke den Domainnamen des zugehörigen PTR-Records analysieren, z.B.: `/\.(a|internet)dsl\.tpnet\.pl$/`

Wie bei allen Anti-Spam-Maßnahmen muss auch hier von Anfang an eine Whitelist vorgesehen werden. In diesem Fall ist sie notwendig, da die ISPs immer wieder die Verwendung der Netze ändern und zum Teil vergessen, diese Änderungen auch zu dokumentieren. Daher müssen sowohl die PBL als auch die regulären Ausdrücke übersteuert werden können.

4.2.2 Reverse DNS-Test

Der Reverse DNS-Test ist ein Konsistenzcheck der Konfiguration im DNS bzgl. der Caller-IP-Adresse und dem zugehörigen Domainnamen. Er besteht aus 3 aufeinander aufbauenden Stufen der Überprüfung:

- Stufe 1: Gibt es zur Caller-IP-Adresse einen zugehörigen Domainnamen, d.h. existiert mindestens ein PTR-Record, der auf einen syntaktisch korrekten Domainnamen zeigt?
- Stufe 2: Gibt es zu jedem der Domainnamen wiederum eine zugehörige IP-Adresse, d.h. existiert jeweils mindestens ein A-Record, der auf eine IP-Adresse zeigt?
- Stufe 3: Stimmt die Caller-IP mit einer der IP-Adressen aus dem A-Record überein?

Wendet man nur den Check der Stufe 1 an, wie dies z.B. die großen ISPs AOL, GMX oder WEB.DE machen, so ist der Test sehr einfach. Es reicht aus, wenn ein PTR-Record existiert.

Wendet man jedoch, wie am LRZ, alle 3 Stufen an, wird es etwas komplizierter, da es sowohl mehrere PTR- als auch A-Records geben kann. Der Test muss jetzt einen Baum konstruieren, bei dem die Wurzel aus der Caller-IP, die Knoten aus den Domainnamen und die Blätter aus den resultierenden IP-Adressen bestehen. Der Test ist in der Theorie dann bestanden, wenn die IP-Adresse aus einem der Blätter mit der aus der

Wurzel übereinstimmt. In der Praxis ist das leider nicht der Fall. Um die Informationen im DNS protokollunabhängig abzufragen, verwenden die meisten MTAs, wie z.B. Postfix, keine eigenen Routinen, sondern benutzen unter Linux die Funktionen getnameinfo bzw. getaddrinfo. Die Funktion getnameinfo gibt aber nur einen Domainnamen zurück, egal wie viele Domainnamen im DNS konfiguriert sind. Da bei jedem Aufruf zyklisch durch die Domainnamen rotiert und damit jedesmal ein anderer Domainname zurück gegeben wird, kann der Fall auftreten, dass der Check einmal funktioniert, beim nächsten Aufruf aber wieder nicht mehr. Wird aufgrund des Checks eine E-Mail mit einem permanenten statt einem temporären Fehlercode zurückgewiesen, so kommen die E-Mails nur manchmal an. Wird hingegen ein temporärer Fehlercode verwendet, so wird eine E-Mail zwar nicht mehr abgewiesen, aber solange verzögert, bis der MTA einen Retry durchführt, bei dem der Check den richtigen Domainnamen bekommt. Die Funktion getaddrinfo hingegen gibt alle konfigurierten IP-Adressen aus, sodass hier dieses Problem nicht auftritt.

Adressen, die den Test nicht bestehen, müssen in eine Whitelist aufgenommen werden, damit die Kommunikation weiterhin aufrechterhalten werden kann.

4.2.3 Greylisting

Anfang 2005 hat sich das LRZ entschieden, Greylisting [19] für *alle* eingehenden E-Mails einzuführen und (damals) als Hauptabwehrmaßnahme gegen Spam zu verwenden. Greylisting ist strenggenommen kein Spamfilter, sondern ein Verfahren zur Identifikation standardkonformer Mailserver.

Das Verfahren setzt darauf, dass sich der *sendende* MTA merken muss, ob die Zustellung einer E-Mail erfolgreich war oder vom empfangenden MTA temporär abgelehnt wurde. Bei einer temporären Ablehnung muss der Sender-MTA nach einiger Zeit versuchen, die E-Mail erneut zuzustellen [10]. Greylisting erzeugt einen temporären Fehler und testet dann einzig und allein für die Eigenschaft *Retry nach einem temporären Fehler*, ob der Zusteller sich wie ein standardkonform implementierter MTA verhält. Es macht daher keinerlei Aussagen darüber, ob der MTA Ham- oder Spammails verschickt.

Technisch wird der Test dadurch realisiert, dass beim ersten Zustellversuch einer E-Mail aus *unbekannter* Quelle die E-Mail temporär zurückgewiesen und in einer Datenbank-Tabelle (Connection Cache) ein Tripel aus der Caller-IP-Adresse, d.h. der IP-Adresse des sendenden MTAs, der Absende- und der Empfangsmailadresse eingetragen wird. Wenn der fremde MTA nach einiger Zeit erneut versucht die E-Mail zuzustellen und eine im Greylisting konfigurierte Wartezeit (14 bzw. 29 Minuten am LRZ) eingehalten hat, so wird diesmal das Tripel im Cache gefunden, die E-Mail angenommen und das Tripel in eine Automatische WhiteList (AWL) übernommen. Wird zu einem späteren Zeitpunkt erneut eine E-Mail mit denselben Daten verschickt, so wird das Tripel in der AWL gefunden, die Quelle ist also nicht mehr unbekannt, und die E-Mail wird sofort entgegengenommen. Zusätzlich wird der Zeitstempel für das letzte Auftreten des Tripels aktualisiert. Dadurch bleibt das Tripel in der AWL solange ein regelmäßiger Mailkontakt besteht. Kommt es nicht zu einem Retry, so wird das Tripel am LRZ nach 24 Stunden aus dem Cache gelöscht. Aus der AWL wird es am LRZ nach 36 Tagen (5 Wochen + 1 Tag) Inaktivität gelöscht.

2005 waren die Botnetze hauptsächlich Proxy-basiert (vgl. Abschnitt 3.1) und hatten die Protokolllogik von SMTP für die Behandlung temporärer Fehlermeldungen nicht implementiert. Zwar könnte Greylisting auch durch eine Wiederholung eines Spamruns nach der Wartezeit leicht ausgehebelt werden, doch auch das war für Proxy-basierte Botnetze nicht einfach zu implementieren, da sie sich die Zuordnung von Caller-IP und Mailadressen hätten merken müssen. Die Bots versandten ihre Nutzlast nach dem „fire and forget“ Prinzip. Sie verhielten sich somit bzgl. der vom Greylisting getesteten Eigenschaft nicht wie korrekt implementierte MTAs. Das ist der Grund für die hervorragende Wirkung von Greylisting als Spamabwehrmaßnahme.

Inzwischen sind aber alle großen Botnetze Template-basiert mit eigener SMTP-Engine. Es wäre also ein leichtes für die Botnetz-Betreiber, eine Replay-Logik oder sogar eine korrekte Behandlung temporärer Fehler einzubauen. Seitdem das LRZ Greylisting einsetzt, ist dies aber nur zweimal der Fall gewesen. Es besteht jetzt aber die Gefahr, dass das Greylisting von einem Tag auf den anderen von einem der Botnetze vollständig ausgehebelt wird und, falls keine anderen Abwehrmaßnahmen in Kraft wären, die LRZ-Relays mit Spammails geflutet würden.

Als Policy Server, der das Greylisting implementiert, wird am LRZ die Software SQLgrey [20] verwendet. Mit dem Einsatz von SQLgrey wird versucht eine möglichste gute Balance zwischen den beiden entgegengesetzten Zielen *Maximierung der Anzahl abgewehrter Spammails* und *Minimierung der Verzögerung der Hammails* zu erreichen. SQLgrey implementiert dazu ein stufenweises Vertrauenskonzept bzgl. des sendenden MTAs. Von Haus aus ist bereits eine Reihe von Maßnahmen in SQLgrey implementiert:

- *Reduktion:* Im Gegensatz zum klassischen Verfahren wird, nach einer korrekten Wiederholung des Zustellversuchs, statt des Tripels <Caller-IP, Absende-, Empfangsmailadresse> nur das Paar <Caller-IP, Absendemailadresse> aus dem Connection Cache in eine automatisch erzeugte Whitelist (from_awl) übernommen. Dadurch wird eine E-Mail, die der Sender an einen weiteren Empänger schickt, sofort angenommen und unterliegt nicht mehr einer anfänglichen Verzögerung.
- *Aggregation:* Sind in die from_awl eine gewisse Anzahl von Datensätzen mit gleicher Caller-IP und Absendedomain (nur die linken Seiten der Adressen unterscheiden sich) eingetragen (10 am LRZ), so wird das Paar <Caller-IP, Absendedomain> automatisch in eine aggregierte Domänen-Whitelist (domain_awl) übernommen. Dadurch, dass der MTA bei mehreren Absendeadressen korrekt einen Retry ausgeführt hat, ist das Vertrauen in diesen MTA gewachsen. Sendet nun *irgendein* Absender dieser Senderdomain über diese Caller-IP eine E-Mail an *irgendwen*, so gibt es keine Verzögerung. In der domain_awl wird die Kenntnis, welcher MTA für welche Domain zuständig ist, gesammelt. Dies kann als eine Art clientbasiertes Sender Policy Framework (SPF) [21] angesehen werden. Sollte das Vertrauen in den MTA so groß werden, dass jede E-Mail angenommen werden soll, so geschieht dies nicht mehr automatisch. Man muss dann die IP-Adresse manuell in die IP-Whitelist eintragen.
- *Throttling:* Werden von einer bisher unbekannten Mailquelle laufend neue Tripel in den Connection Cache aufgenommen, so sinkt mit jedem weiteren Tripel das Vertrauen in diese Mailquelle. Ab einem Schwellwert (20 am LRZ) muss zuerst ein korrekter Retry für eines der Tripel im Cache erfolgen bevor weitere Tripel akzeptiert werden. Dadurch wird

die Wahrscheinlichkeit reduziert, dass eine zufällige Wiederholung eines Tripels als ein korrekter Retry gewertet wird.

Um Verzögerungen bei der Annahme von E-Mails zu minimieren, sollten Einträge möglichst schnell von der from_awl in die domain_awl aggregiert werden. Würde z.B. der Aggregationslevel auf 1 gesetzt, so würde bereits nach der *ersten* eventuell zufälligen Wiederholung jeder Eintrag direkt in die domain_awl wandern. Dadurch würde aber die Kontrolle, ob ein MTA vertrauenswürdig ist, stark gelockert werden. Das LRZ ist einen anderen Weg gegangen. Um ein hohes Vertrauen in den sendenden MTA zu gewinnen, wurde der Aggregationslevel vom Default 2 auf 10 erhöht. Um trotzdem eine Minimierung zu erreichen, wurde eine Reihe von Erweiterungen implementiert, bei denen zusätzliche Kriterien herangezogen wurden, um auch bei wenigen Einträgen in der from_awl (3 statt 10) eine Domain in die domain_awl übernehmen zu können. Die wichtigsten sind:

– *SPF-Check:* Hat die Absendedomain einer E-Mail im DNS einen SPF Record (Sender Policy Framework), der besagt, dass der Client autorisiert ist, E-Mails für diese Domain zu versenden, so reicht dies als zusätzliches Indiz für einen regulären MTA aus.
– *MX-Check:* Wird zum Versenden und Empfangen einer Domain der gleiche MTA benutzt, so ist dies ebenfalls ein zusätzliches Indiz für einen regulären MTA.

Auch im Bereich der AWLs wurden Erweiterungen programmiert. Für Delivery Service Notifications (DSN) wurde eine eigene AWL (dsn_awl) angelegt, da diese Einträge nie zur Aggregierung herangezogen werden können und daher die from_awl nur belasten.

Eine Analyse der Einträge in der from_awl ergab, dass es in einigen Fällen eine große Menge an Tripel gab, die sich nur durch die Absendeadressen unterschieden. Diese Tripel resultieren in der Regel aus Forwards von fremden MTAs an Adressen im MWN, wobei auf diesem Wege sehr viele Spammails hereinkommen. Da die Absenderadressen der Spammails gefälscht sind und meist nur einmal genutzt werden, entsteht eine große Menge an Datensätzen, die die from_awl „verschmutzt“. Da die E-Mails von regulären MTAs kommen, werden durch das Greylisting auf beiden Seiten unnötig Ressourcen vergeudet. Es wurde daher eine weitere AWL implementiert (rcpt_awl), in die für solche Fälle automatisch das Paar <Caller-IP, Empfangsadresse> aufgenommen wird

4.2.4 Überprüfung der Empfangsadressen

Wie viele Mailrelays für große Intranets haben früher auch die LRZ-Relays alle E-Mails, die durch die Spamabwehr gelangten, angenommen und weitergeleitet, ohne bereits an dieser Stelle zu überprüfen, ob der Empfänger überhaupt existiert. Grund dafür ist in der Regel, dass die Relays nicht wissen, welche Adressen gültig sind, da diese Information nur bei den End-Systemen vorhanden ist. War die empfangene E-Mail eine Spammail und existierte der Empfänger nicht, so wurde von den Relays eine Backscatter-Spammail erzeugt und verschickt.

Damit die LRZ-Relays nichtBackscatter erzeugen, wenn der Empfänger nicht existiert, wurde damit begonnen, den Relays die notwendigen Informationen zu Verfügung zu stellen. Die Benutzerverwaltung der Message Stores wurde vollständig auf LDAP-Directorys umgestellt. Die Relays können somit über LDAP jede vom LRZ verwaltete Mailadresse auf Gültigkeit überprüfen. Für die vielen lokalen Mailserver im MWN, für die in der Regel kein LDAP-Server zur Verfügung steht, verwenden die LRZ-Relays die Möglichkeit, über einen SMTP-Callout [22] die Adressen zu prüfen. Das Ergebnis wird zur Performance-Verbesserung in einem Cache-Dämon zwischengespeichert. Da ein SMTP-Callout sehr aufwändig ist – es wird für jede Adressüberprüfung eine extra E-Mail erzeugt und versucht, diese an den Ziel-MTA zu übertragen – kann dieses Verfahren nur für MTAs mit geringem E-Mail-Verkehr durchgeführt werden.

Mit der Empfängerüberprüfung kann zwar die größte Quelle an Backscatter vermieden werden, Backscatter aufgrund von Abwesenheitsmeldungen wird aber weiterhin erzeugt, da zurzeit alle durch die Abwehr geschlüpften Spammails in der zweiten Phase nur markiert und anschließend zugestellt werden.

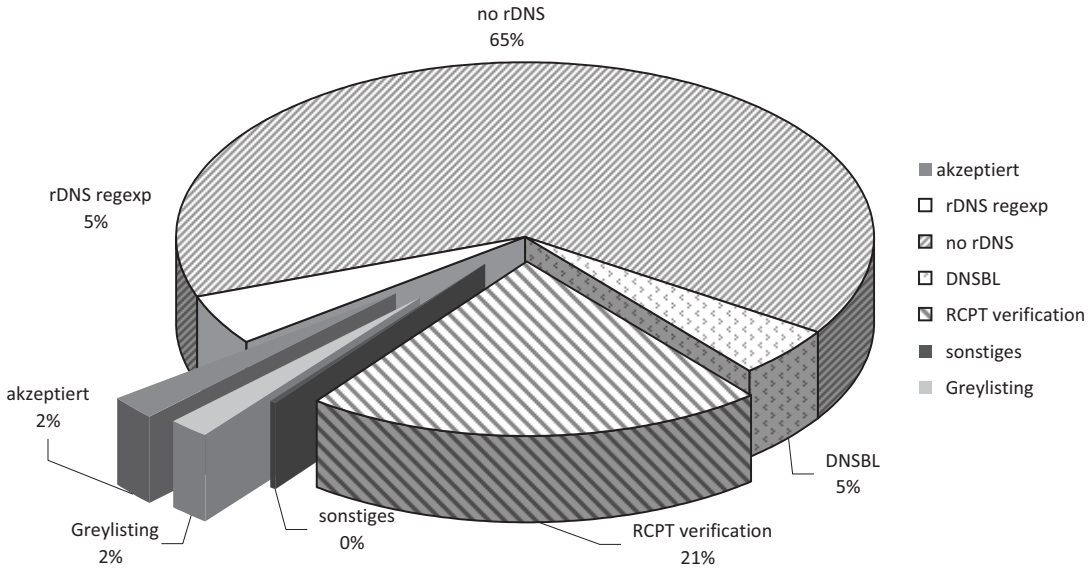

Abb. 3 Abgelehnte E-Mails im Monat Mai 2008

5 BETRIEBSERFAHRUNGEN

Im – insbesondere im Vergleich zum Jahresende 2007 – ruhigen Monat Mai 2008 wurden insgesamt 76 Millionen Zustellversuche registriert, was einer Durchschnittsrate von etwa 1800 E-Mails pro Minute entspricht. Dieser niedrige Wert wird jedoch bei Botattacken über Stunden hinweg um den Faktor 10 überschritten, dabei belegen die angreifenden Bots trotz starker Limitierungen bis zu 1500 parallele Serverprozesse.

Einen Löwenanteil der Abweisungen machen die rDNS-basierten Prüfungen aus (s. Abb. 3). 49 Millionen und damit 65% bestehen bereits die erste Prüfung, den PTR/A-Konsistenzcheck nicht, weitere 5% werden durch einen regulären Ausdruck als Dialup klassifiziert und abgewiesen. 16 Millionen (21%) E-Mails werden bei der Überprüfung der Empfängeradresse abgewiesen, eine Annahme hätte unweigerlich zum Versand der entsprechenden Anzahl DSNs geführt („Backscatter"). Durch den Einsatz der DNSBL werden weitere 5% dauerhaft abgewiesen. 2% werden durch das Greylisting-System temporär abgewiesen.

Am Ende wurden von 76 Millionen Versuchen nur 1,9 Millionen (2,5%) E-Mails zur deutlich aufwändigeren weiteren Verarbeitung angenommen.

Im Folgenden werden die Betriebserfahrungen, die mit den verschiedenen vorgestellten Maßnahmen gemacht wurden, vorgestellt.

5.1 Greylisting

Am 22.02.2005 wurde Greylisting aktiviert. Die Wirkung war hervorragend, wie Abb. 4 zeigt:

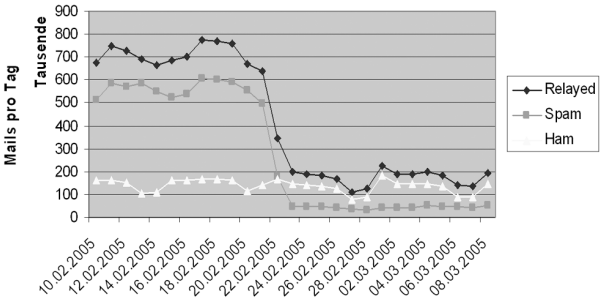

Abb. 4 Anzahl angenommener Spam- und Hammails bei der Einführung von Greylisting

Man sieht deutlich, wie die Anzahl an angenommenen Spammails sinkt während die Anzahl der Hammails den gleichen Wochenrhythmus wie vor der Einführung zeigt.

Bei der Einführung des Greylistings wurde versucht, die Einschwingzeit für die Verzögerung der Hammails so klein wie möglich zu halten Es wurden daher vor der Inbetriebnahme die Logfiles der LRZ-Relays über 5 Wochen ausgewertet und alle Tripel zu den empfangenen E-Mails, egal ob Ham oder Spam, zusammen mit dem Zeitpunkt des letzten Auftretens in die AWLs eingetragen. Da nach 36 Tagen Inaktivität ein Tripel aus der AWL gelöscht wird, alterten die zu viel eingetragenen „Spam"-Tripel zum größten Teil in den 5 Wochen nach Inbetriebnahme heraus, da sie nur einmalig genutzt wurden. Außerdem wurde eine umfangreiche manuelle Whitelist für große ISPs angelegt. Sie umfasst inzwischen ca. 400 IP-Adressen und ca. 250 IP- Netze.

Wie man der Abb. 5 entnehmen kann, begannen wir mit einem Anteil an verzögerten E-Mails von nur 11% statt 100% und waren innerhalb von 2 Wochen unter die 5% Marke gerutscht. Danach blieb der Wert bereits mit den Standardverfahren von Sqlgrey relativ konstant bei nur 3%. Durch die Einführung der LRZ-Erweiterungen zur schnelleren Übernahme von Einträgen aus der form_awl in die domain_awl konnte die Rate der verzögerten Hammails bis auf ca. 1,5% gedrückt werden. Die Verzögerung selbst bewegt sich, bedingt durch unsere Konfiguration, in der Regel im Bereich von 30 bis 60 Minuten.

Der Betrieb an sich ist erfreulich wartungsarm, ein Management der Autowhitelists ist unnötig. Fälle, in denen eine E-Mail nicht zugestellt werden konnte, weil der sendende Mailserver nicht standardkonform war, traten am Anfang ungefähr einmal pro Woche, später einmal pro Monat auf. Sobald wir darauf aufmerksam gemacht wurden und die IP-Adresse bekannt war, konnte das Problem schnell durch einen Eintrag in die Whitelist gelöst werden.

Bisher wurde das Greylisting zweimal ausgehebelt:

- Im März 2006 trat ein Botnetz in Erscheinung, dessen Spambots im Zeitraum von 20 Minuten alle 5 Minuten ein Retry durchführten. Um dieses Problem zu beheben, genügte es, die Wartezeit für Erstkontakte von 14 auf 29 Minuten zu erhöhen.
- Die Pennystock-Spams des Botnetzes SpamThru schlugen ab November 2006 durch Replay der Spam-Attacke immer wieder voll durch (vgl. Abb. 6) und hörten erst auf, als die U.S. Securities and Exchange Commission (SEC) im März 2007 gegen den Handel von 35 Penny Stocks vorging [23].

Mitte 2007 kam es zu Performanceproblemen durch die brute force Angriffe eines Botnetzes (vgl. Abb. 7). Bei 1 Million E-Mails pro Stunde war die Grenze unseres MySQL-Servers, auf dem die AWLs lagen, erreicht. Als Bottleneck stellte sich der

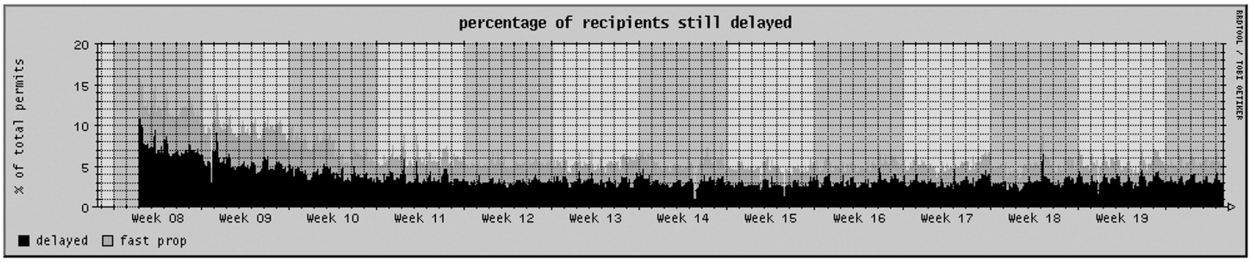

Abb. 5 Verzögert zugestellte E-Mails (delayed) ab der Einführungswoche von Greylisting

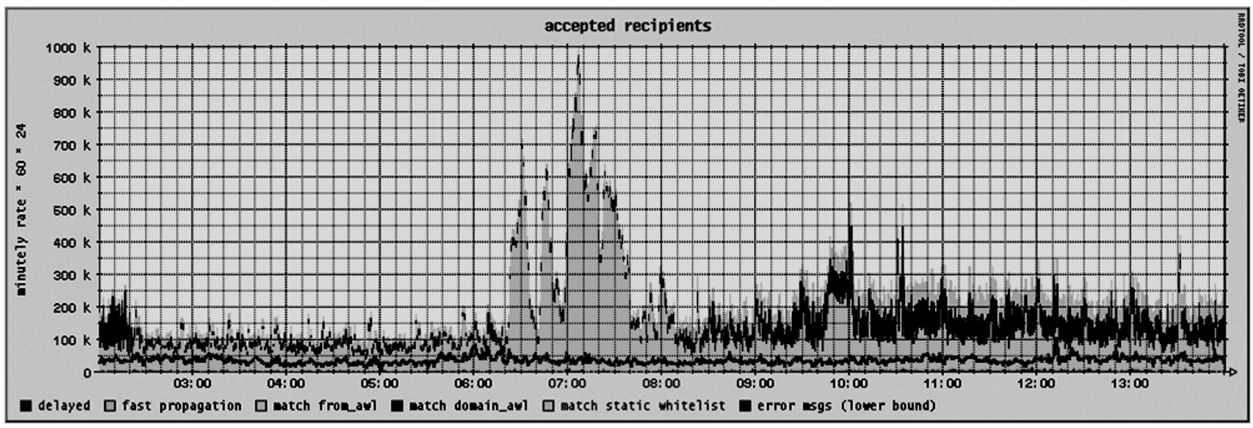

Abb. 6 Erfolgreiche Attacke durch Replay

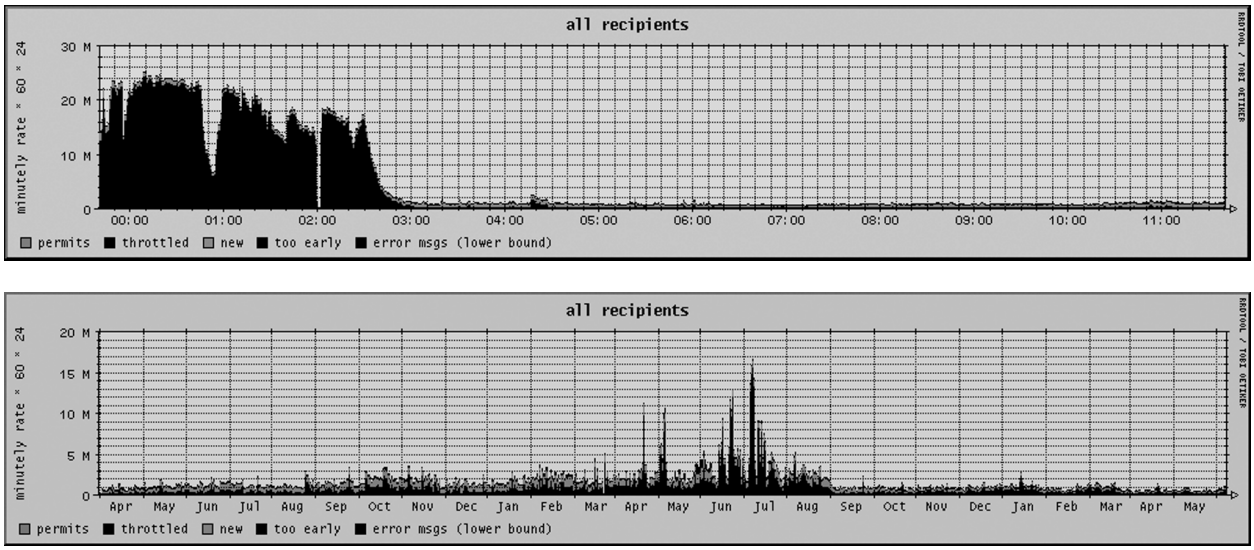

Abb. 7 Erfolglose brute force Attacken im Sommer 2007 (ca. 1 Million E-Mails pro Stunde)

Datenpfad zwischen Speicher und CPU heraus. Ein Umstieg auf neuere Hardware hätte die Grenze um den Faktor 2,7 erhöht.

Wegen der Performanceprobleme und der Gefahr, dass Greylisting doch plötzlich ausgehebelt werden könnte, wurden ab September 2007 die bereits beschriebenen zusätzlichen Anti-Spam-Maßnahmen vor das Greylisting gesetzt. Die Entlastung des Greylistings ist in der Abb. 7 deutlich zu erkennen.

Fazit: Greylisting war das erste rein formale, nicht den Inhalt der E-Mails inspizierende Verfahren und als solches ausgesprochen erfolgreich. Es lässt sich auch heute noch sinnvoll und erfolgreich einsetzen, falls es von geeigneten Maßnahmen ergänzt wird. Für die Konfiguration am LRZ spielt es inzwischen eine untergeordnete Rolle.

5.2 Reverse DNS-Test

Wie bei jeder Anti-Spam-Maßnahme stellt sich auch beim Reverse DNS-Test die Frage nach dem Anteil an regulären MTAs, die dadurch abgewiesen werden. Da die Überprüfung nach Stufe 1 (vgl. Abschnitt 4.2.2) inzwischen von einigen großen ISPs eingesetzt wird, ist davon auszugehen, dass die Anzahl der fälschlich abgewiesenen MTAs relativ gering ist. Auf der anderen Seite sollte sich der Mangel (falsche DNS-Konfiguration) durch den Administrator des MTAs recht schnell beheben lassen, wenn es doch zu einer Abweisung kommt.

Um die Effizienz zu testen, wurde der Stufe-1-Check mit in den Greylisting Policy Server eingebaut. Es zeigte sich, dass damit bereits bis zu 40% der sonst vom Greylisting geblockten E-Mails abgewiesen wurden.

Um auch die Stufe 3 evaluieren zu können, wurde ein MTA basierend auf Postfix aufgebaut, über den eine größere Domain geroutet wurde, wobei die Stufe 3 nur im Testmodus betrieben und nur entsprechende Meldungen ins Log geschrieben, die E-Mails aber nicht zurückwiesen wurden. Überraschenderweise konnte damit die Ablehnungsrate zeitweise auf bis zu 80% gesteigert werden. Im Monatsschnitt wurden immer noch 65% erreicht. Gleichzeitig stieg aber die Anzahl der regulären MTAs, die wegen falscher Konfiguration abgewiesen wurden, rasant an. Grund dafür ist die äußerst nachlässige Administration der Daten bzgl. der IP-Adressbereiche im DNS durch die jeweiligen ISPs. Die Folge ist, dass auf der einen Seite die Ablehnungsrate hervorragend hoch ist und auch nicht von den Spammern

beeinflusst werden kann, auf der anderen Seite aber auch die Daten regulärer MTAs im DNS falsch konfiguriert sind.

Um festzustellen, welche MTAs durch diese Maßnahme betroffen wären, wurden alle IP-Adressen, von denen die Relays E-Mails entgegennahmen untersucht. Dazu wurden aus den Greylisting-AWLs ca. 100.000 IP-Adressen extrahiert und dem Konsistenz-Check mit Hilfe eines dafür entwickelten Scripts unterzogen. Mehr als 8% der IP-Adressen schafften den Check nicht. Durch manuelle Inspektion der Liste und den zugehörigen Statistikdaten aus den AWLs konnte der Wert auf 5,5% gedrückt, der Rest der IP-Adressen, als von Bots gekapert, identifiziert werden.

Da der Wert mit 5,5%, also 5.500 Whitelist-Einträgen, doch weit über den Erwartungen lag, haben wir uns erst nach intensiver Diskussion dazu entschlossen, diese Maßnahme bei einigen der größten Maildomains in Produktion einzusetzen. Es war zu befürchten, dass es trotz der großen Whitelist, die durch obige Untersuchung entstand, zu vielen Supportfällen und Nachträgen in der Whitelist kommen würde. Dies war erfreulicherweise nicht der Fall. Ähnlich wie beim Greylisting trat am Anfang nur ein Supportfall pro Woche auf.

5.3 Backscatter

Welchen Ärger Backscatter-Spam machen kann, weiß man erst, wenn man einmal selbst Opfer davon war. Im Januar 2008 fanden ca. 30 Nutzer im MWN, als sie aus dem Weihnachtsurlaub wieder an die Arbeit zurückkehrten, tausende von „Spams“ in ihrer Mailbox vor. Ein Spammer hatte ihre Mailadressen als Absender für seine Viagra-Spammails verwendet. Mitte April waren auf einmal mehrere Hundert Mailadressen betroffen, unter anderem auch die Mailadressen fast aller LRZ-Mitarbeiter. Im Mai wechselte der Spammer erneut seine Mailadressen und das Problem verschwand für das LRZ.

Um diesen Nutzern wieder ein Arbeiten zu ermöglichen, wurden Filter konfiguriert, um die Fehlermeldungen (DSNs) dieses Spammers soweit wie möglich zu blockieren.Von Januar bis April wurden insgesamt weit über 1 Million diese Backscatter-Spammails durch unsere Filter erkannt, im Schnitt mehr als 30.000 pro betroffenen Nutzer. Die Filter konnten aber nur solche DSNs erkennen, in denen auch Teile der ursprünglichen Spammail enthalten waren. DSNs ohne Anhaltspunkt, sowie die ganzen automatisch erzeugten Antworten, schlugen voll auf die Mailboxen durch. Nach groben Schätzungen kamen auf 30 ausgefilterte DSNs ein DSN und eine weitere automatische Antwort durch die Filter.

Dieser Vorfall führte dazu, so schnell wie möglich flächendeckend die Empfangsadressen bereits an den LRZ-Relays zu überprüfen – um nicht selbst zur Verbreitung von Backscatter beizutragen. Es fehlt aber weiterhin an Möglichkeiten, auch die automatischen Antworten zu unterdrücken.

6 AUSBLICK

Das hier vorgestellte Maßnahmenbündel ist zurzeit sehr effektiv; dabei ist es relativ einfach und Ressourcen-schonend zu implementieren.

Im Moment ist die organisierte Kriminalität im Internet auf dem Vormarsch – auf der anderen Seite sind die PCs von Endanwendern nach wie vor gefährdet. Oft werden sie durch Drive-By Infektionen gekapert, ohne dass der Anwender es merkt. Aus diesen Gründen bleiben Botnetze ein Thema – entsprechend wachsen die Kapazitäten der Spammer weiter. Doch nicht nur quantitativ machen die Spammer Fortschritte. Wie der bisherige Verlauf des Kampfes zwischen Spammern und Mailadministratoren gezeigt hat, werden Spammer nach und nach neue Methoden entwickeln, um die gängigen Schutzmaßnahmen auszuhebeln.

In der Zwischenzeit können die Abwehmaßnahmen weiter ausgebaut werden. Mögliche Bereiche sind:

- Aufbau einer Webschnittstelle, über die ein fehlkonfigurierter MTA direkt durch den betroffenen Sender, Empfänger oder Administrator in die Whitelist eingetragen werden kann, ohne dass manuell eingegriffen werden muss. Um einen Missbrauch zu verhindern kann eine Rückkopplung über die inhaltliche Analyse der Phase 2 erfolgen. Sobald das Verhältnis von Spam zu Ham einen Schwellwert überschreitet, wird die entsprechende Adresse aus der Whitelist entfernt und kann nicht mehr direkt freigeschaltet werden. Es lassen sich dadurch weitere Restriktionen und Checks schneller einführen, da bei Blockaden die Betroffenen selbst aktiv werden können.
- Schnittstellen für den Endkunden bereitstellen, über die er feststellen kann, welche E-Mails von der Spamabwehr zurückgewiesen wurden. Dadurch ist es für ihn einfacher, false positives festzustellen und über obige Webschnittstelle für die Zukunft zu verhindern.
- Implementation eines Moduls zur automatischen Benachrichtigung von Administratoren über Fehlkonfigurationen. Je stärker die Anzahl der falsch konfigurierten System verringert werden kann, desto einfacher können die vorgestellten Maßnahmen zur Spamabwehr einsetzt werden.

Eine Organisation muss ihre Anti-Spam-Strategie an ihren Möglichkeiten ausrichten. Wer wenig Manpower oder keine IT-Security Kernkompetenzen hat, aber dafür über genug Kapital verfügt, sollte erwägen, externe Dienstleister in Anspruch zu nehmen – die dann in der Pflicht stehen, mit den Entwicklungen Schritt zu halten. Wer darauf angewiesen ist, sich selbst durch einen innovativen Methodenmix zu schützen – muss seine Vorgehensweise immer wieder anpassen und darf dabei auch die unsichere und noch in Veränderung befindliche Rechtslage nicht aus den Augen verlieren.

7 LITERATURVERZEICHNIS

[1] Leibniz-Rechenzentrum: Das Leibniz-Rechenzentrum. [Online] http://www.lrz-muenchen.de/wir/intro/de/.

[2] Leibniz-Rechenzentrum: Das Münchner Wissenschaftsnetz (MWN) – Konzepte, Dienste, Infrastrukturen, Management. [Online] 2006. http://www.lrz-muenchen.de/services/netz/mwn-netzkonzept/mwn-netzkonzept.pdf.

[3] Leibniz-Rechenzentrum: Leibniz-Rechenzentrum – Auf einen Blick. [Online] http://www.lrz-muenchen.de/home/.

[4] Leibniz-Rechenzentrum: E-Mail am LRZ. [Online] http://www.lrz-muenchen.de/services/netzdienste/email/.

[5] Leibniz-Rechenzentrum: Jahresbericht 2007. [Online] 2008. http://www.lrz-muenchen.de/wir/berichte/Jber2007.pdf/Jber2007.pdf.

[6] Ironport: Spammers Continue Innovation: IronPort Study Shows Image-based Spam, Hit & Run, and Increased Volumes Latest Threat to Your Inbox. [Online] 2006. http://ironport.com/company/ironport_pr_2006-06-28.html.

[7] Wikipedia: Botnet. [Online] http://de.wikipedia.org/wiki/Botnet.

[8] Stewart, Joe: Top Spam Botnets Exposed. [Online] 2008. http://www.secureworks.com/research/threats/topbotnets/?threat=topbotnets.

[9] Marschall: Spam Statistics. [Online] http://www.marshal.com/trace/spam_statistics.asp.
[10] Klensin, John (Eds.): Simple Mail Transfer Protocol. s.l.: IETF, 2001. RFC 2821.
[11] Wikipedia: Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). [Online] http://de.wikipedia.org/wiki/Captcha.
[12] Wikipedia: Challenge-response spam filtering. [Online] http://en.wikipedia.org/wiki/Challenge-response_spam_filtering.
[13] Leibniz-Rechenzentrum: Windows Server Update Service (WSUS) für Windows 2000/XP/2003 des LRZ. [Online] 2008. http://www.lrz-muenchen.de/services/security/mwnsus/.
[14] Leibniz-Rechenzentrum: Die Anti-Virus Seite des LRZ. [Online] http://www.lrz-muenchen.de/services/security/antivirus/.
[15] Fliegl D.; T. Baur; H. Reiser u. B. Schmidt: Ein generisches Intrusion Prevention System mit dynamischer Bandbreitenbeschränkung. 20. DFN-Arbeitstagung über Kommunikationsnetze. Heilbronn: s.n., 2006.
[16] (ICSI), International Science Foundation. Bro Intrusion Detection System. [Online] http://www.bro-ids.org/.
[17] Gellens, Randall und Klensin, John: Message Submission. s.l.: IETF, 1998. RFC 2476.
[18] Spamhaus: The Spamhaus Project. [Online] http://www.spamhaus.org/.
[19] Harris, Evan: The Next Step in the Spam Control War: Greylisting. [Online] 2003. http://projects.puremagic.com/greylisting/whitepaper.html.
[20] Bouton, Lionel: SQLgrey. [Online] http://sqlgrey.sourceforge.net/.
[21] Wong, M. und Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1. s.l.: IETF, 2006. RFC 4408.
[22] Postfix Address Verification Howto. [Online] http://www.postfix.org/ADDRESS_VERIFICATION_README.html.
[23] U.S. Securities and Exchange Commission: SEC Suspends Trading Of 35 Companies Touted In Spam Email Campaigns. [Online] 2007. http://www.sec.gov/news/press/2007/2007-34.htm.