Greylisting schützt vor Wurm-generierten Spam-Mails

Verzögerungstaktik

Wirkungsvoller Schutz vor Spam muss mit immer neuen Tricks der Müllversender Schritt halten. Derzeit aktuell: Spam-versendende Würmer. Gegen sie hilft Greylisting: Der Empfänger lässt den Sender kurz warten. Echte Mailserver kümmert das kaum, nur Spammern fehlt das Durchhaltevermögen. Peer Heinlein

Die Welle der E-Mails kam überraschend aus dem Nichts und war unüblich heftig. Binnen weniger Stunden prasselte Anfang Juni 2004 auf E-Mail-Nutzer eine Welle vermeintlicher Leserbriefe und Zeitungsartikel nieder, die sich bei näherem Hinsehen als rechtsradikale Propaganda herausstellte.

Abgesehen vom politisch motivierten Inhalt ließen sich diese Aussendungen in die lange Liste des üblichen elektronischen Werbemülls einordnen. Sie offenbarten jedoch, welche Arbeitsmittel die Spammer künftig nutzen werden: Massenhaft infizierte Desktop-PCs, die durch einen Wurm oder Virus zur Spamschleuder mutieren, siehe Kasten „Spammer sind Würmer".

Die Gilde der Postmaster schlägt zurück und entwickelt neue Techniken, um den Tricks der Spammer beizukommen. In den letzten Monaten zeichnen sich aus den vielen Ideen vier zukunftsweisende Ansätze ab, siehe Kasten „Spam-schutz-Strategien". Doch nicht alle sind einsatzreif und empfehlenswert. Neben technischen Schwierigkeiten sind auch lizenzrechtliche Probleme zu befürchten, wenn einzelne Firmen ihre Lösung in den Markt drücken.

Wirkt gegen Spam-Würmer

Besonders trickreich arbeitet Greylisting [1], das gezielt die Schwächen der primitiven Spamschleudern ausnutzt. Es gehört zwar zur Gruppe von Strategien und Techniken, die nur den Empfang von Spam blocken, aber nicht den Versand verhindern. Dennoch bewährt es sich als schlagkräftige Waffe im Kampf mit der dunklen Seite des Netzes.

Die Idee ist ebenso einfach und trivial wie genial. Der auf den Massenversand optimierten Spamsoftware fehlt ebenso wie Viren und Würmern ein wichtiger Mechanismus echter Mailserver: Temporär unzustellbare E-Mails verwerfen sie einfach, statt sie wie ein MTA zwischenzulagern, um später erneute Zustellversuche zu unternehmen. Das Ziel der Spammer ist ja nicht, zuverlässig jede Nachricht auszuliefern, sondern möglichst viele Mails in kurzer Zeit abzusetzen. Da lohnt es nicht, sich um einzelne Problemfälle gesondert zu kümmern.

Ein Mailserver, der Greylisting anwendet, speichert bei jeder ankommenden E-Mail das folgende Triple zusammen mit der aktuellen Uhrzeit:

- Mailadresse des Absenders
- Mailadresse des Empfängers
- IP-Adresse des einliefernden Hosts

Anschließend gibt der MTA einen temporären Fehler »4*xx*« aus. Wie der Ablauf einer entsprechenden SMTP-Sitzung genau aussieht, zeigt Abbildung 1.

Anders als bei permanenten Fehlern der »5*xx*«-Klasse wird es ein abgewiesener Mailserver nach einer Wartezeit von wenigen Minuten erneut versuchen, die Mail zuzustellen. Bei jedem weiteren Versuch erkennt der empfangende Mailserver, dass die Datenbank bereits ein passendes Triple enthält. Nach Ablauf eines Zeitfensters – viele Admins setzen die Wartezeit auf 15 Minuten – nimmt der MTA die Mail an und stellt sie dem Empfänger zu.

Die ebenso nüchterne wie erfolgreiche Logik: Viren und Spamprogramme unternehmen mangels Mailqueue keine weiteren Zustellversuche. Schon ist die Quelle der Mails geblockt. Leider hat

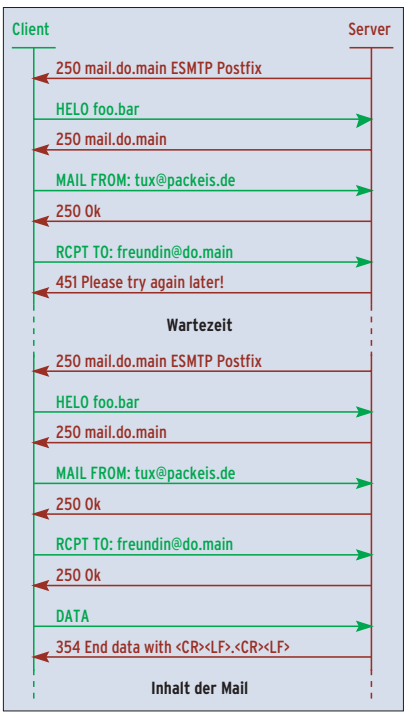

Abbildung 1: Je nachdem, ob die Wartezeit des Triple abgelaufen ist oder nicht, antwortet der Mailserver auf »RCPT TO:« mit Response-Code 451 oder 250.

auch Greylisting einige Nebenwirkungen. Das größte Problem ist, dass jede ankommende Mail um mindestens 15 Minuten verzögert eintrifft. Das mag zwar in den meisten Fällen unproblematisch sein, ruft im Einzelfall aber den Unmut der Nutzer hervor.

Mit etwas Fleiß kann der Admin dieses Problem minimieren, wenn er unverdächtige Mailserver über eine Ausnahmeliste vom Greylisting befreit. Es gibt bereits gemeinsam gepflegte Whitelisting-Listen [7]. Ein Großteil des Mailverkehrs fließt dann wieder verzögerungsfrei. Die meisten Mailversender nutzen eine überschaubare Anzahl großer Provider, die ihre Server recht gut gegen Missbrauch sichern.

Eine Greylisting-Maschine ist sogar lernfähig, wenn sie bekannte Triples nach der Wartezeit und Freischaltung noch mehrere Stunden oder Tage in ihrer Datenbank aufbewahrt. Jede weitere E-Mail dieses Briefwechsels passt auf das bekannte Triple und darf ohne Wartezeit passieren. Kommunizieren zwei User täglich, werden sie keine Verzögerungen mehr feststellen (Abbildung 2).

In der Praxis gibt es aber Probleme. So fehlt vereinzelt auch legitimen Mailservern eine Mailqueue – die Server von Yahoogroups gehören in diese Kategorie. Sie verwerfen bei einem temporären »4*xx*«-Fehler die Mails an ein Listenmitglied und verzichten auf erneute Zustellversuche. Aber das Problem ist lösbar: Entweder ändert Yahoogroups seine Strategie oder jeder Greylist-Betreiber trägt diese regelwidrigen Server in eine Whitelist ein.

Einige MTAs prüfen die Absenderadresse von E-Mails dadurch, dass sie eine kurze SMTP-Sitzung zum Mailserver der

Spammer sind Würmer

Heutige Viren und Würmer laden auf infizierten Rechnern neuen Code von Internetservern nach und erhalten dadurch auch nach ihrer Verbreitung neue Aufgaben und Programmfunktionen. In auffallend gleichem Maße, wie die Verbreitung der rechten E-Mails zunahm, sanken die Infektionsversuche des E-Mail-Wurms Sober.G auf nahezu null.

24 Stunden nach Beginn der Spamaktion wurde fast kein Exemplar des Wurms mehr im Internet verschickt: Alle von ihm infizierten PCs waren mit dem Versand der Spam-Mails beschäftigt, nachdem ihnen ein Remote-Update die neue Aufgabe zugewiesen hatte. Damit bestätigte sich der schon länger gehegte Verdacht, dass Spamversender und Virenautoren entweder identisch sind oder zumindest Hand in Hand arbeiten. Wurmprogrammierer bieten ihre Produkte sogar als Dienstleistung auf dem Markt an.

Wenn sich ein Wurm gut verbreiten konnte, steht denen, die ihn zu kontrollieren wissen, ein mehrere Millionen Installationen umfassendes Heer zur Verfügung und damit eine immense Rechenleistung und Netzwerkkapazität. Was damit im Guten möglich ist, das zeigen die Leistungen der auf Desktop-PCs verteilten Rechensysteme bei Seti at Home [5] oder bei der gemeinsamen Suche nach Mersenne-Primzahlen [6].

Greylisting für Postfix

Für alle bekannten MTAs sind mittlerweile gute Implementierungen verfügbar, zum Beispiel für Postfix, Sendmail, QMail und Exim. Manchmal ist die Implementierung in den MTA schwierig, da Greylisting neue Schnittstellen zur MTA-Software benötigt. Bei Postfix ist mindestens Version 2.1 nötig, da erst sie die erforderlichen Policy Services [9] kennt.

Skript und Datenbank bremsen Spammer

Die Hauptarbeit erledigt das Perl-Skript »greylist.pl«, das dem Postfix-Quellcode und verschiedenen Distributionen beiliegt. Im Skript selbst sind eventuell Anpassungen nötig. Meist genügt es, die vorgesehene Blockierdauer von 60 auf 15 Minuten zu reduzieren und den Pfad zur Datenbank zu korrigieren, etwa auf »/var/mta/greylist.db«. Dieses Verzeichnis und die Datenbank müssen für den User »nobody« beschreibbar sein. Die »master.cf« muss noch folgenden Eintrag für den Policy-Dienst enthalten:

```
policy  unix  -  n  n  -  -  spawn
user=nobody  argv=/usr/bin/perl
/usr/lib/postfix/greylist.pl
```

Außerdem ist der »main.cf« der Timeout des Policy-Dienstes hoch anzusetzen. Das erledigt die Zeile:

```
policy_time_limit=3600
```

Danach kann man das Greylisting in die Restrictions-Prüfungen von Postfix aufnehmen. Vorzugsweise an passender Stelle in den »smtpd_recipient_restrictions«: Hier entscheidet Postfix, ob es eine E-Mail entgegennimmt oder nicht. Die genaue Platzierung des Eintrags hängt von der existierenden Prüflogik ab. Eine mögliche Grundkonfiguration könnte wie folgt aussehen, entscheidend ist die letzte Zeile:

```
smtpd_recipient_restrictions =
  permit_mynetworks,
  permit_sasl_authenticated,
  reject_unauth_destination,
  check_policy_service unix:private/policy
```

Domain des Absenders starten (SMTP Callback) und dabei prüfen, ob dieser Server die Absenderadresse als Empfänger akzeptieren würde. Benutzt der Absender Greylisting, scheitert sein Test zunächst am absichtlichen temporären Fehler. Damit verzögert sich auch das Versenden der eigenen Mails.

Für den Callback verwenden die meisten Server eine leere Absenderadresse. Erkennt ein Greylist-Server einen Null-Absender, wartet er mit seiner Fehlermeldung bis nach dem »DATA«-Befehl. Zu diesem Zeitpunkt haben die rücküberprüfenden MTAs ihre SMTP-Sitzung erfolgreich beendet, während Spammer immer noch in die Falle tappen.

Auch große Provider mit einer ganzen Farm versendender Mailserver könnten in Schwierigkeiten geraten, wenn jeder erneute Zustellversuch von einer neuen IP-Nummer aus geschieht. Abhilfe schafft hier die Idee, die Triples anhand eines Class-C-Netzes statt einzelner IP-Nummern zu betrachten. Die Maschinen einer Mailserver-Farm arbeiten meist im selben Netzbereich.

Schwierige Maillisten

Noch nicht ganz gelöst ist ein Problem mit der Mailinglisten-Software Ezmlm, die für jede E-Mail eine einmalige Absenderadresse erzeugt. Ezmlm schafft es damit, Bounces (automatisch generierte Antwortmails) der auslösenden Mail zuzuordnen. Jedoch hat damit jede Mail ein neues Triple und Greylisting wird jede E-Mail erneut ausbremsen. Abhilfe schaffen hier ein manuelles Whitelisting von Ezmlm-Servern oder eine langfristige Änderung bei Ezmlm. Der bei Greylisting problemlos funktionierende Mailinglisten-Manager Mailman zeigt, dass diese Dienste auch ohne Tricks mit Absenderadressen auskommen.

Keines dieser Probleme ist unlösbar. Der Zusatzaufwand durch Workarounds bleibt klein im Vergleich zu dem Ärger, den andere Spam-Schutzmaßnahmen mit sich bringen. Vor allem die False Positives herkömmlicher Spamfilter ärgern die User: Wenn der Filter echte E-Mail fälschlicherweise als Spam deklariert und dauerhaft blockt, dann gerät der Schutz gelegentlich zum größeren Problem als der Spam selbst. Bei Greylisting beschränken sich False Positives auf Mailverluste von fehlerhaft implementierten Mailservern.

Erste Auswertungen über den Erfolg von Greylisting lassen selbst erfahrene Administratoren staunen. False Positives traten zum Beispiel an der TU Chemnitz nicht auf, die Verzögerungen erwiesen sich nach einer kurzen Trainingsphase

Spamschutz-Strategien

Derzeit werden mehrere Ansatzpunkte für wirksamen Schutz vor Spam diskutiert und weiterentwickelt.

Greylisting: Diese Mischung aus White- und Blacklisting nutzt die Tatsache, dass Spamsoftware und Viren meist keine vollständige SMTP-Engine enthalten. Greylisting ist ausgereift, gut implementierbar, zieht keine hohe Serverlast nach sich und hat keine False Positives. Nachteil: E-Mails werden teilweise verspätet ausgeliefert. Die Methode bekämpft leider nur Symptome, nicht aber die Ursachen (mehr dazu im Artikel). [1]

Sender Policy Framework: SPF setzt auf die längst vorhandene Infrastruktur der DNS-Server auf. Es definiert in den »TXT«-Records einer Domain, welcher Server als offiziell genutzter Mailserver für ausgehende E-Mail dient. Damit ist SPF gewissermaßen das Gegenstück der MX-Records eingehender E-Mail. Das verhindert, dass Spammer die Absenderadresse fälschen. Das Verfahren lässt sich recht leicht umsetzen.

Für den Absender bedeutet SPF, dass er stets über den Provider seiner Domain relayen muss. Datenschützer und politische Netzkämpfer wittern hier Missbrauchsmöglichkeiten. Das größte Problem ist aber, dass SPF das Weiterleiten von Mails verhindert. Forwarding führt dazu, dass E-Mails eines Absenders von einem fremden Mailserver verbreitet werden. Mit der heutigen Praxis im Mailverkehr ist SPF daher schlecht vereinbar. [2]

Microsoft Sender ID: Basiert auf der gleichen Idee wie SPF und definiert ebenfalls in DNS-Records die für ausgehende Mail zuständigen Server einer Domain. Anders als SPF sorgt die MS-Caller-ID jedoch für vergleichsweise hohe Serverlast, da sie die Informationen über komplizierte XML-Strukturen in den DNS-Records ablegt. Neben der Tatsache, dass Mailserver in der Regel kein XML beherrschen, könnten sich lizenzrechtliche Probleme gegenüber Microsoft ergeben. [3]

Yahoo Domain Keys: Hier muss der Mailserver ausgehende Mails mit einem festgelegten Schlüssel seiner Domain signieren und die Signatur in den Header der Mail einbetten. Andere Mailserver erfahren den Public Key der Senderdomäne per DNS und können anhand der Signatur prüfen, ob die E-Mail ordnungsgemäß vom zuständigen Server transportiert wurde. Allerdings erzeugen die Verschlüsselungsalgorithmen eine hohen Serverlast und es tritt – ebenso wie bei SPF – das Problem auf, dass alle Nutzer über fest definierte Mailserver versenden müssten. [4]

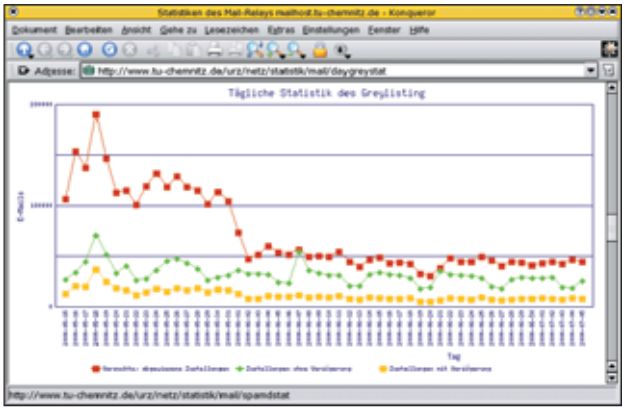

Abbildung 2: An dieser Statistik der TU Chemnitz ist deutlich zu sehen: Nach kurzer Trainingszeit verzögert das Greylisting nur noch wenige erwünschte E-Mails (gelb), bei gleichzeitig guten Filter-Erfolgen (rot).

als unproblematisch und der Server wurde kaum belastet [8]. „Wir hatten wahnsinnig gute Effekte“, schwärmt Frank Richter, Postmaster der TU Chemnitz. „Das Spam-Aufkommen reduzierte sich so deutlich, dass besorgte Nutzer anriefen und fragten, ob der Mailserver defekt wäre.“

Langfristig ist aber auch mit Greylisting der Kampf gegen Spam noch keinesfalls gewonnen. Der Postmaster erreicht nur einen vorübergehenden Vorteil, solange sich Spammer und Virenprogrammierer nicht auf diese Abwehrmaßnahme einstellen und Queueing-Mechanismen in ihre Software implementieren. Wie bei allen Verfahren, die Symptome statt Ursachen bekämpfen, gilt auch hier: Beim gegenseitigen Wettrüsten liegt mal die eine, mal die andere Seite vorn.

Der zusätzliche Aufwand für Spammer, um auch das aufwändige Queueing zu implementieren, gibt den Postmastern einen guten Vorsprung. Sie sollten diesen Vorteil auch nutzen. *(fjl)*

Infos

[1] Greylisting: [http://projects.puremagic.com/greylisting/]
[2] Sender Policy Framework: [http://spf.pobox.com]
[3] Microsoft Sender ID: [http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx]
[4] Yahoo Domain Keys: [http://antispam.yahoo.com/domainkeys]
[5] Seti at Home: [http://setiathome.ssl.berkeley.edu]
[6] Mersenne-Primzahlen-Suche: [http://www.mersenne.org/prime.htm]
[7] Whitelisting: [http://greylisting.org/whitelisting.shtml]
[8] Greylisting an der TU Chemnitz: [http://www.tu-chemnitz.de/urz/mail/filter/greylist.html]
[9] Greylist-Policy für Postfix: [http://www.postfix.org/addon.html#policy]