Antispam-Appliance mit Langzeitwirkung

Spezialfilter

Mailserver müssen auch ohne Spam und E-Mail-Würmer genug arbeiten. Diesen störenden Ballast dauerhaft aus dem Datenstrom zu filtern, ist das erklärte Ziel des SMTP-Proxyservers Sponts. Das Gerät soll sogar die Empfängeradresse aus den Mailinglisten der Spammer entfernen. Der Test klärt, ob und wie das funktioniert. Tobias Eggendorfer

Die kleine Sponts-Box, etwa so groß wie ein aufeinander gestapelter Jahrgang Linux-Magazine, will ein kleines Wunder vollbringen und die Spamflut dauerhaft eindämmen [1]. Die Box fungiert als SMTP-Proxy zwischen dem bisherigen SMTP-Server und dem Internet. Im SMTP-Dialog prüft sie jede eingehende Mail und weist Spam sofort zurück. Ein Trick soll dafür sorgen, dass Spammer die Sponts-geschützten Empfänger nicht weiter belästigen.

Trickreiche Theorie

Die Idee ist simpel: Je öfter der Spammer eine Mail an eine bestimmte Adresse nicht senden konnte, desto eher wird er diese Adresse löschen. Die Herstellerfirma IKU nennt das den Sponts-Effekt [1]. Da die Sponts-Box die Annahme bereits im SMTP-Dialog verweigert, ist die bei Spam meist gefälschte Absenderadresse unerheblich. Der Proxy präsentiert direkt dem versendenden Rechner die Fehlermeldung. Dadurch erfährt der Spammer, dass sein Werbemüll nicht zugestellt werden konnte. Ganz anders als bei einem Protest-Antwortschreiben, das in den meisten Fällen an unbeteiligte Dritte gehen würde.

User verleugnen

Der SMTP-Proxy der IKU-Entwickler verschweigt in der Fehlermeldung, dass ein Spamfilter die Mail aussortiert hat. Er meldet vielmehr, dass der Empfänger nicht existiert: »User unknown«. Für den Spammer bleibt der Filter unsichtbar und er kann nicht durch Ausprobieren herausfinden, wie er ihn am besten umgeht. Manche Antispam-Tools geben dem Absender detaillierte Informationen, warum sie die Mail als Spam klassifiziert haben. Das ist kostenlose Schulung zum Umgehen der Filter.

Die »User unknown«-Meldung im SMTP-Dialog ist plausibel und für einen Spammer auch automatisiert auswertbar. Er könnte die Adressliste seiner Opfer also um diesen Eintrag kürzen, denn einen gelöschten Account beliefern frisst nur Bandbreite ohne jede Erfolgsaussicht. Andere Meldungen zeigen in der Regel nur ein temporäres Problem an, bei dem es sich nicht sofort anbietet, die Adresse zu löschen.

Begrenzte Erfolgsaussicht

Funktionieren kann der Trick aber nur, wenn das Spam-Opfer seine Adresse anschließend nicht mehr im Web publiziert [3] oder nur noch in verschlüsselter Form darstellt [2]. Andernfalls landet der geblockte Account schon beim nächsten Spider-Durchlauf wieder in den Listen der Spammer.

In der Theorie klingt das Verfahren überzeugend. Zweifelhaft ist, ob der Effekt wirklich so schnell eintritt, wie der Hersteller IKU in einer Grafik [1] darstellt. Der Autor dieses Artikels hat im April 2004 einen stark bespammten Mail-Ac-

Sponts-Box

Produkt: Sponts-Box

Hersteller: IKU [http://www.iku-ag.de]

Bauform: Mini-ITX (295 x 270 x 61 mm) mit externem Netzteil oder 19-Zoll-Gehäuse (1 HE)

Anwendung: Antispam-Appliance, als SMTP-Proxy ausgeführt

Filtermethoden: Backend-Check, RBL (Real-time Black List), Sender Domain SMTP Check, RFC 821 und 822 Strict, Black- und Whitelisting, Spamassassin

Gerätepreis: 570 Euro (Mini-ITX) oder 820 Euro (19-Zoll-Gehäuse).

Lizenzkosten: Grundsoftware 420 Euro (für 10 Postfächer) bis 3950 Euro (1000 Postfächer), Zusatzmodule je nach Zahl der Fächer und Modul einmalig 285 Euro bis 5300 Euro [11]

count deaktiviert, der Mailserver gab danach im SMTP-Dialog immer »User unknown« zurück. Die Auswertung der Logfiles ergab, dass der Server im April täglich 90 Mails zurückgewiesen hat, Mitte Juni 2004 waren es immer noch täglich im Mittel über 60. Die Menge hat sich in sechs Wochen auf etwa zwei Drittel reduziert. Immerhin ähnelt die Tendenz der IKU-Grafik. Der Unterschied kann an Zufällen liegen – es ist kaum vorhersagbar, wann welcher Spammer welchen Account erwischt.

Zu mitteilsam

Bei der praktischen Umsetzung der Theorie zeigt sich der erste Mangel: Die Sponts-Box meldet sich im SMTP-Dialog mit »220 SPONTS v1.1.1 SMTP ready« und ist damit für jeden Spammer identifizierbar. Er könnte gezielt alle »User unknown«-Meldungen dieser Box ignorieren, der Zusatzaufwand wäre minimal. Damit entfiele der Sponts-Effekt. Die Box sollte besser die Standardmeldung eines bekannten SMTP-Servers oder eine neutrale Nachricht senden.

Zudem meldet Sponts nicht immer »User unknown«, sondern teilweise auch »User unknown for you« oder schlimmer »554 -- You are blacklisted«, sodass nur bei einem Teil der gefilterten Mails tatsächlich die Voraussetzungen für die erhoffte Wirkung gegeben sind.

Wie stark der Effekt dann tatsächlich eintritt, hängt vor allem von der Qualität der Spamfilter ab. Die Box benutzt mehrere Filterstufen. Für jeden Regelverstoß kann der Admin einstellen, dass die Box die Mail sofort abweisen soll (siehe Abbildung 2). Weitere Regeln prüft sie dann nicht mehr. In der Praxis erweist sich dieses Vorgehen als ungünstig, da die Tests einzeln wenig aussagekräftig sind. Günstiger ist es, den Gesamt-Spamscore als Kriterium zu nehmen und den Schwellenwert so zu konfigurieren, dass mindestens zwei Filter mit hoher Wahrscheinlichkeit Spam vermuten müssen.

Zu spät

Leider darf ein Mailserver nach dem »DATA«-Kommando im SMTP keine »User unknown«-Meldung mehr senden (siehe Kasten „Der SMTP-Dialog"). Die abschließende Bewertung ist aber erst möglich, wenn der SMTP-Proxy den Inhalt der Nachricht kennt, also nach dem »DATA«-Kommando. Wenn Sponts eine Mail zu diesem Zeitpunkt aussortiert, muss es sich offenbaren.

Damit geht der Sponts-Effekt verloren. Es gäbe hierfür allerdings eine Lösung: Die Box könnte nach dem E-Mail-Empfang einen temporären Fehler melden und sich die Kombination aus Absender und Empfänger merken – ähnlich wie beim Greylisting (siehe Artikel in der Sysadmin-Rubrik). Beim nächsten Zustellungsversuch wüsste Sponts schon vor dem »DATA«-Kommando, dass sie Spam erhält, und könnte rechtzeitig mit »User unknown« reagieren. Im Test zeigte die Appliance leider nichts in dieser Richtung.

Eine gute Chance verschenkt die Software auch, wenn ein Sender aus der schwarzen Liste auftaucht: Sie meldet ihm direkt, dass er auf eben dieser Liste steht: »504 You are blacklisted«. Hier ließe sich im SMTP-Dialog noch plausibel ein »User unknown« verpacken.

Mehrere Filterstufen

Sponts verwendet folgende Techniken, um Spam zu erkennen:

- Backend-Check
- RBL (Realtime Black List)
- Sender Domain SMTP Check
- RFC 821 und 822 Strict
- Black- und Whitelisting

Der Backend-Check ist kein Spamtest im strengen Sinn. Er prüft lediglich, ob der eigene Mailserver eine Mail mit diesem Adressaten akzeptieren würde.

Bei RBL (Realtime Black List) handelt es sich um permanent aktualisierte Listen von offenen Relays und offenen Proxys. Spammer missbrauchen diese Systeme gern, um ihren Müll weiterleiten zu lassen. Die RBLs verfolgen zwei Ziele: Jede Mail, die über ein Open Relay kommt, ist dringend Spam-verdächtig. Außerdem zwingt der RBL-Einsatz die Provider, ihre offenen Relays nach Kundenbeschwerden zu schließen. Allerdings gibt es immer wieder Pannen, beispielsweise landete GMX mehrfach auf schwarzen Listen [5], [6]. Eine RBL allein ist nicht ausreichend zuverlässig.

Sponts nutzt auf Wunsch zwar mehrere RBLs, gewichtet die Einzelergebnisse aber gleich. Während manche RBLs zuverlässig arbeiten, bezeichnen sich andere noch als experimentell und aggressiv [7]. Um das aufzufangen, könnte man zum Beispiel ein Spamcop-Listing nur mit einem Punkt gewichten und einen Ordb.org-Eintrag mit vier Punkten.

Der SMTP-Dialog

Eine E-Mail besteht aus einem Envelope – eine Art virtueller Briefumschlag – und der Nachricht selbst. Auf dem Umschlag stehen die Adressen des Absenders und des Empfängers. Sie müssen nicht zwangsläufig identisch sein mit den Adressen in »To:«- und »From:«-Feldern des Nachrichtenheaders. Das ist sogar sinnvoll, ein BCC funktioniert so.

Diese Umschlagadressen teilt der Absender im SMTP-Dialog mit (Abbildung 1), zuerst die Absenderadresse »MAIL FROM:*Sender@Example.Com*«, danach die des Empfängers »RCPT TO:*Someone@Example.Com*«. Die Nachricht selbst folgt anschließend nach dem Schlüsselwort »DATA«.

Ein Mailserver darf, sobald er den Empfänger kennt, die Zustellung ablehnen, etwa weil er sich nicht für zuständig erachtet oder der Empfänger nicht existiert. Im Prinzip ist es sogar möglich, mit dieser Begründung die Mail erst nach dem Übertragen der Nachricht abzulehnen. Allerdings ist das im SMTP nicht erwünscht. In der Regel soll ein Mailserver nach der Nachricht nur noch Fehlermeldungen wie »account over quota« oder »message to long« ausgeben – diese Ereignisse kann er aber vorher noch nicht ahnen [12].

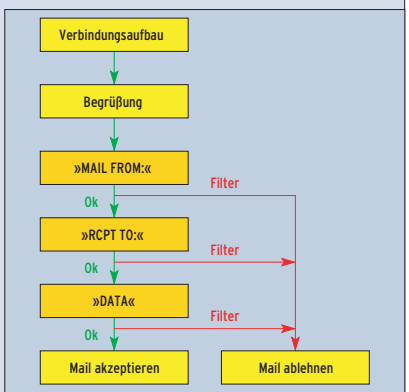

Abbildung 1: Im Ablauf des SMTP-Dialogs kann der Mailserver an mehreren Stellen unauffällig Fehlermeldungen generieren, die dem Absender falsche Tatsachen vorspielen. Damit will die Sponts-Box Spammer dauerhaft vertreiben.

Günstiger scheint da der Sender Domain SMTP Check: Sponts überprüft in dieser Stufe, ob für die Absenderdomain ein MX-Eintrag existiert und ob der Mailserver der Domain Mails mit dieser Adresse annimmt. Auf diese Weise lassen sich frei erfundene Mailadressen leicht entarnen. Der Haken dabei: Spammer gehen dazu über, die Mailadresse eines unbeteiligten Dritten als Absender einzutragen, um diesen Test zu bestehen.

Gültiger Absender

Viele Mailserver melden mittlerweile auf einen SMTP-Verify nicht mehr, ob die Adresse tatsächlich existiert. Sie prüfen nur die korrekte Schreibweise und ob der Server für die Domäne zuständig ist. Das soll verhindern, dass Spammer durch schnelles Ausprobieren ganze Listen gültiger Adressen generieren. Der Domain-Check ist lediglich ein nettes Add-on, das Anfängern unter den Spammern das Leben etwas erschwert. Leider verursacht der Test zusätzlichen Traffic. Ähnlich ist der Test auf RFC-Konformität der Absenderadresse zu bewerten. Statt Spammer-Tricks zu bemerken, entdeckt dieser Test vor allem Mails von schlecht implementierten Clients und löst falschen Spam-Alarm aus. Außerdem sollte sich der Test statt auf RFC 822 auf den aktuelleren RFC 2822 [8] beziehen.

Spamassassin unter Wert

Zusätzlich kann Sponts die Mails durch Spamassassin [4] filtern lassen. Allerdings ist es nicht möglich, den mit diesem Tool erkannten Spam sofort abzuweisen, das Ergebnis erhöht nur den Gesamt-Spamscore. Das Testgerät bot auch keine Möglichkeit, Spamassassin zu konfigurieren, der Admin darf diesen Test nur ein- oder ausschalten.

Dabei ließe sich gerade Spamassassin bei der Contentanalyse hervorragend tunen. In Produktivumgebungen ist das auch nötig: Eine Online-Apotheke sollte andere Spamscores für Viagra vergeben als eine Großbank. Auch bei der Header-Analyse ließe sich Spamassassin an die eigene Umgebung anpassen, um die Filterqualität deutlich zu erhöhen. So neigen Spammer zunehmend dazu, ihren Werbemüll über einen Mail-Exchange niedrigerer Priorität zu liefern.

Der Autor lässt Spamassassin in den Headerzeilen prüfen, ob die Mail von seinem Reserve-MX angenommen wurde, und erhöht dann den Spamscore geringfügig. Gerade bei Filter-optimiertem Spam ist das oft der entscheidende Hinweis. Fällt der Primary-MX aus, müssten die Filter diese Regel wieder rausnehmen. Allerdings wäre das ausgefallene Gerät dann gerade die Sponts-Box.

Administration

Die Filteraktionen lassen sich gut nachvollziehen, Sponts generiert sehr ausführliche Logfiles. Dort ist klar zu erkennen, warum die Software welche Mail wie beurteilt hat. Schade ist jedoch, dass man die Logs nur per SFTP herunterladen kann und nicht per Webinterface oder SSH. Gerade beim Testen der Konfiguration wäre ein »tail -f« praktisch. Der fehlende SSH-Zugang erwies sich im Test als lästig: Die Weboberfläche gibt nicht auf alle Funktionen Zugriff, sie ist

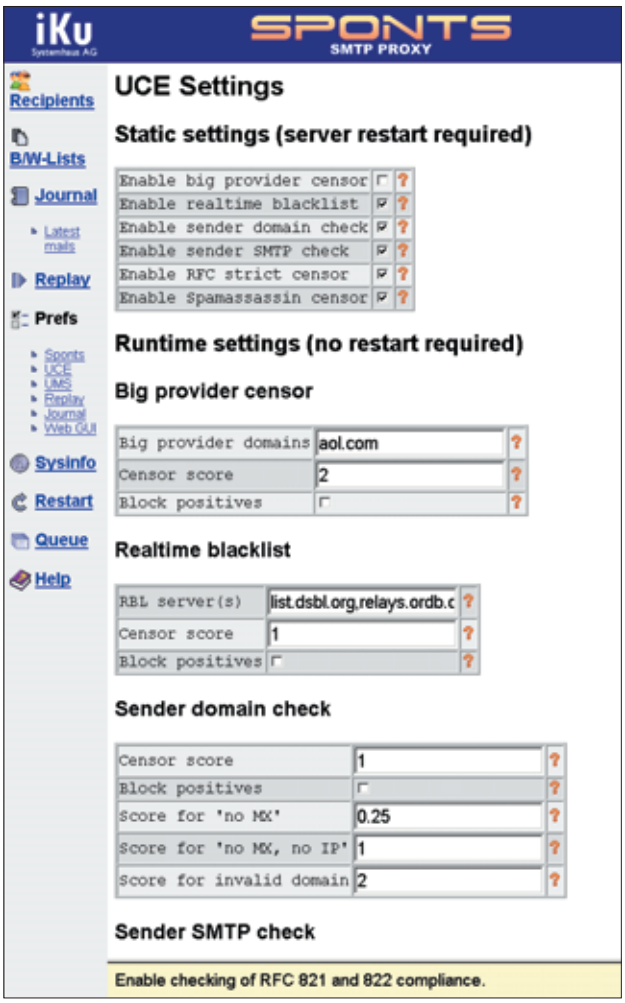

Abbildung 2: Bei jedem Spamfilter kann der Admin wählen, ob Sponts die Mail sofort abweist (»Block positives«) oder vorerst nur den Gesamt-Spamscore erhöht (»Censor score«). Den Big-Provider-Sensor will IKU demnächst ersetzen.

Abbildung 3: Die Sponts-Box muss wissen, für welche Empfänger oder Empfängerdomänen der SMTP-Proxy arbeiten soll. Dem Admin steht dafür leider nur ein einzeiliges Textfeld in der Weboberfläche zur Verfügung.

teilweise umständlich zu bedienen und ihr fehlen wichtige Tools.
Der Admin muss zunächst alle Domains und Mailadressen eintragen, für die Sponts E-Mail empfangen soll (Abbildung 3). Dazu steht ihm aber nur ein einzeiliges Input-Feld zur Verfügung. Angenehmer wäre ein Bulk-Add oder die Möglichkeit, etwa die »virtusertable« von Sendmail hochzuladen. Wer MySQL beherrscht, umgeht mutig dieses Manko: Er verbindet sich direkt auf Port 3306 und manipuliert die Datenbank mit den Adresslisten. Jedoch ist die Datenbankstruktur nicht dokumentiert.
Den direkten MySQL-Weg benötigte der Autor auch nach einem Tippfehler: Er hatte statt @ versehentlich ein Euro-Symbol eingegeben und zu schnell auf Speichern geklickt. Bei der zehnten eingetragenen Adresse ein nicht ganz unwahrscheinlicher Fehler. Über das Webinterface war das nicht zu korrigieren, da das Euro-Symbol nur verstümmelt auf der Box ankam und die Adresse selbst als Primärschlüssel in der internen Datenbank dient. Hier wäre eine Eingabevalidierung in der Webapplikation hilfreich gewesen.
Auch beim Versuch, den Nameserver-Eintrag der Box über das Webinterface zu korrigieren, scheiterte der Tester. Hier stoppte ihn ein HTTP-500-Fehler. Ein weiteres Manko ist das Installieren des Lizenzschlüssels: Statt über das Webinterface ist der Schlüssel umständlich und mit höherem Fehlerrisiko über SFTP auf die Box zu laden.

Weboberfläche mit Schwächen

Diese Mängel ließen einen Root-Login auf die Box vermissen. Bei einer Appliance wirkt dieses Anliegen zwar ungewöhnlich, bei einem unausgereiften und umständlichen Webinterface wäre ein Remote-Login aber sehr hilfreich. Zahlreiche Funktionen, die sich in einem nicht dokumentierten Config-File verstecken, lassen sich über die Weboberfläche nicht aktivieren. Das Handbuch rät dem Nutzer dringend ab, selbst die Konfigurationsdatei zu manipulieren.
Dass das Webinterface noch Mängel hat, scheint auch dem Hersteller bewusst zu sein. Das Handbuch weist explizit auf die Möglichkeit hin, die Datenbanken direkt zu manipulieren, ohne jedoch die Datenstruktur zu beschreiben.
Schade auch, dass die Box offenbar für den Einsatz hinter der Unternehmens-Firewall gedacht ist. Wer mehrere Mailserver unterschiedlicher Priorität verwendet, muss jeden durch Sponts schützen. Mindestens ein niederpriorer MX steht meist nicht im eigenen Rechenzentrum, sondern extern, um auch beim Totalausfall der hausinternen Infrastruktur noch Mails entgegenzunehmen.

Keine Firewall

In der externen Umgebung läuft die Firewall meist auf dem SMTP-Server. Sponts stünde hier offen und gefährdet. Da wäre es wichtig, per Webinterface IP-tables-Firewallregeln zu konfigurieren. Nur wenige Ports müssen auf dem SMTP-Proxy geöffnet sein, das Interface wäre daher recht einfach. Leider hat IKU dieses Feature nicht vorgesehen. Schön wäre auch, wenn die Box einen HTTP-Proxy für den Download der Virensignatur-Updates benutzen könnte. Wer bereits die Antiviren-Software von H+BEDV einsetzt, würde damit Traffic-Kosten sparen. Die Virenerkennung selbst funktionierte im Test übrigens sehr gut und zuverlässig.
Laut Dokumentation ist Sponts nur für den Empfang von E-Mail zuständig, nicht für das Ausliefern von Mails an externe Domänen. Da der MX-Eintrag im DNS auf die Sponts-Appliance zeigen muss, führt dies zu einem weiteren Problem: Der versendende Mailserver ist laut DNS nicht der für die Domäne zuständige Host. Das könnte Spamfilter in den Empfängerdomänen dazu verleiten, die Nachrichten als Spam einzustufen.

Gastkommentar: User unknown im Selbstbau

Wer Postfix als Mailserver benutzt, kann RBL-geblockte Mails sehr einfach mit »User unknown« abweisen. Normalerweise lautet die Konfiguration:

```
default_rbl_reply = $rbl_code Service ➥
  unavailable; $rbl_class [$rbl_what]
blocked using $rbl_domain${rbl_reason?; ➥
  $rbl_reason}
maps_rbl_reject_code = 554
```

Ändert man diese Einträge in der »main.cf«, dann serviert Postfix bei RBLs eine ähnliche Meldung wie die Sponts-Box:

```
default_rbl_reply = $rbl_code
<${recipient}>: ➥
  User unknown in local recipient table
maps_rbl_reject_code = 550
```

Ich halte es aber für problematisch, die Meldungen zu verdrehen, da RBL auch viele nicht-spammende Nutzer erfasst. Im herkömmlichen Fall sagt ihnen eine Bounce-Mail, wo das Problem liegt. Erzeugt der Mailserver stattdessen ein »User unknown«, werden viele Anwender Probleme haben, die Ursache zu verstehen. Ich selbst würde das nicht auf meinen Servern so aktivieren wollen: Die Klagen, Fragen und Beschwerden („Wieso ist das unzustellbar, gestern ging's und später ging's auch …") würden mein Support-Team und mich wahrscheinlich schlichtweg platt machen. ***(Peer Heinlein, Autor des Postfix-Buchs)***

Einige Kinderkrankheiten

Im Vergleich mit der Dokumentation fanden sich im Testgerät einige Unstimmigkeiten: So war ein Zugriff über HTTPS auf das Webinterface nicht möglich. Der sehr leichtgängige und aus dem Gerät herausragende Powertaster führte im Test öfter zu unplanmäßigen Arbeitspausen. Anders als dokumentiert schaltet er sofort und nicht erst nach vier Sekunden. Eine Funktion für einen geordneten Shutdown war überhaupt nicht vorhanden, nur ein Reset ließ sich über das Webinterface auslösen.
Lästig ist auch, dass die Weboberfläche einen grafikfähigen Browser erfordert, der mit Frames umgehen kann. Der in vielen Serverräumen verbreitete Lynx ist damit überfordert. Mit Mozilla 1.2 unter KDE funktionierte die Onlinehilfe nicht. Erst nach einem Update auf 1.6 war dieses Problem gelöst.
Sehr angenehm an dem System: Es gibt keine beweglichen Teile. Als Festplatte fungiert eine 256 MByte große IDE-Flashkarte. Ein passiver Kühlkörper genügt, um den Via-C3-Prozessor bei Laune zu halten. Das Testsystem verfügte unerklärlicher Weise über USB- und Parallelports sowie Sound-Ausgänge (siehe Abbildung 4). Ohne Root-Login konnte der Tester das Gerät aber nicht dazu bewegen, bei jeder geblockten Spam-Mail „Heureka" zu rufen. In dem

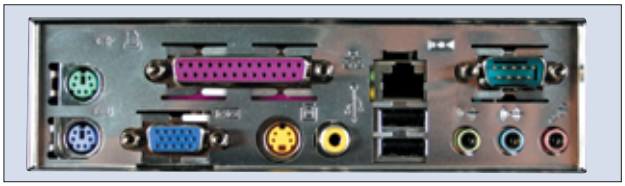

Abbildung 4: Die Rückansicht der Box zeigt für eine Appliance ungewöhnlich viele Buchsen. USB-, Parallel- und Sound-Anschlüsse bleiben derzeit ungenutzt, die aktuelle Software-Release greift nicht auf sie zu.

Abbildung 5: Der Innenraum der Sponts-Box wirkt aufgeräumt und übersichtlich. Es wäre sogar noch ausreichend Platz vorhanden, um das externe Netzteil künftig ins Innere der Appliance zu verlagern.

kleinen Minit-ITX-Gehäuse selbst bleibt noch viel Platz (Abbildung 5). So viel, dass das externe Netzteil leicht hineingepasst hätte. Ein Teil weniger, das jetzt nur rumliegt.

Die Box läuft unter einer angepassten Debian-Version; IKU entwickelte die Software komplett in Java. Der integrierte POP3-Server ist jedoch offenbar noch fehlerhaft, während des Tests hinterließ er im Logfile eine »Java.lang.NullPointerException«.

Mit dem POP3-Server soll es möglich sein, Mails direkt vom SMTP-Proxy abzuholen, wenn der dahinter liegende Mailserver ausfällt. Sponts verfügt dazu über einen Puffer, der die letzten eingegangenen Mails zwischenspeichert. Eine Replay-Funktion stellt die gepufferten Mails auf Wunsch auch erneut an den internen Server zu. Diese Backup-Funktion kann sich in der Praxis als sehr nützlich erweisen.

Fazit

Sponts verwendet innovative Ideen im Kampf gegen Spam. Ein Filter, der sich nicht zu erkennen gibt und dessen Ziel es ist, E-Mail-Adressen aus den Listen der Spammer zu streichen, ist optimal. Allerdings vergibt die Box einige gute Chancen, indem sie zum Beispiel bei einem Blacklisting eine zu informative Nachricht ausgibt. Auch sonst bleibt sie in der getesteten Version hinter ihrem Potenzial zurück, da die Konfigurationsmöglichkeiten nicht ausreichen. Das Webinterface wirkt unausgereift.

Durch ihren Prüfaufwand arbeitet die Box recht langsam. Das Einliefern normalgroßer E-Mails dauert selbst über ein 100-MBit-Netz häufig länger als eine Sekunde. Damit besteht die Gefahr, dass die Box schnell überlastet wird und der Admin sie deaktivieren muss. Dieses Problem ist in größeren Umgebungen mit anderer Hard- und Software bereits bekannt [9], [10].

Die Lizenzkosten [11] für den Spamfilter richten sich nach der Zahl der zu verwaltenden Postfächer und liegen zwischen gut 400 Euro pro Jahr für zehn Postfächer und knapp 4000 Euro jährlich für 1000 Fächer. Für die Replay-Funktion und den Mailpuffer fallen zusätzliche Kosten in etwa derselben Größenordnung an, sie sind allerdings nur einmalig zu entrichten. Die Hardware kostet im kleinen Mini-ITX-Gehäuse 570 Euro, im 19-Zoll-Rackgehäuse 820 Euro.

Mehrfach-Investition

Um sicher zu filtern, muss Sponts vor jedem Mailserver installiert werden. In größeren Netzen mit Mailservern an verschiedenen Standorten sind dazu mehrere Geräte nötig. Damit erhöhen sich die Anschaffungs-, Lizenz- und Wartungskosten, eventuell kommen noch Rack-Mieten in externen Rechenzentren hinzu. Wer diesen recht hohen Aufwand nicht scheut und auf eine Softwareversion warten kann, die die angesprochenen Schwachstellen behebt, hat eine potente Waffe im Kampf gegen Spam. Die aktuelle Version vergibt leider viele gute Chancen. *(fjl)* ■

Infos

[1] Sponts-Box: [http://www.iku-ag.de/produkte/sponts.jsp]
[2] Tobias Eggendorfer, „Privatadresse – Homepage spamsicher gestalten“: Linux-User 05/04, S. 42
[3] Center for Democracy and Technology, „Why am I getting all this spam?“, 2003: [http://www.cdt.org/speech/spam/030319spamreport.pdf]
[4] Spamassassin: [http://www.spamassassin.org]
[5] Holger Bleich, „GMX landet auf Open-Relay-Blacklist“: [http://www.heise.de/newsticker/meldung/37138]
[6] Urs Mansmann, „Spamcop sperrt GMX“: [http://www.heise.de/newsticker/meldung/40206]
[7] Spamcop-Blacklist: [http://www.spamcop.net/bl.shtml]
[8] RFC 2822, Internet Message Format: [http://www.ietf.org/rfc/rfc2822.txt]
[9] Michael Kurzidim, „E-Mail-Server der Bundesregierung nahezu lahm gelegt“: [http://www.heise.de/newsticker/meldung/47526]
[10] Hans-Peter Schüler, „Spam-Welle überrollt die TU Braunschweig“: [http://www.heise.de/newsticker/meldung/47575]
[11] Sponts-Preisliste: [http://www.iku-ag.de/produkte/Preisliste_SPONTS.pdf]
[12] RFC 2821, Simple Mail Transfer Protocol: [http://www.ietf.org/rfc/rfc2821.txt]

Der Autor

Tobias Eggendorfer [http://www.eggendorfer.info] ist in München als freiberuflicher IT-Berater und Dozent tätig. Er freut sich immer, wenn er Spammer ärgern kann. Schlecht konfigurierte Spamfilter dagegen bringen ihn auf die Palme.