Anti-Spam-Tricks mit Linux

Spam und Viren in E-Mails sind zwar aufgrund der härteren Strafen für Spammer in den USA insgesamt etwas rückläufig, dennoch liegt der Spam-Anteil in mancher Mailbox noch immer über 70 %. Zum Glück hält die Open-Source-Community manches Gegenmittel bereit. Wir stellen Ihnen mit „MailCleaner" eine auf die Bekämpfung von Spam und Viren spezialisierte Lösung vor, mit der Sie unerwünschte E-Mails direkt am Internet-Gateway blockieren (Thomas Zeller)

MailCleaner versteht sich als so genannte Appliance und bringt neben Debian Linux 3.1 als Betriebssystem auch alle Tools zum Filtern von Spam und Viren mit. Dazu gehören ClamAV Antivirus, Greylisting, heuristische Spam-Identifikationstechniken (Bayes-Filter) sowie diverse Blacklists. MailCleaner verfügt darüber hinaus über eine optische Zeichenerkennung (OCR), mit der auch so genanntes Image-Spam zuverlässig erkannt wird.

Was kann MailCleaner?

Wie bei Appliances üblich ist für die Installation ein dediziertes System erforderlich – MailCleaner wird also nicht auf dem Client oder einem Mailserver installiert, sondern erwartet seine eigene Systemumgebung. Dafür kommt praktisch jede x86-kompatible Hardware mit Gigahertz-CPU, mindestens 512 MB RAM und 10 GB freiem Plattenplatz in Frage. Das gilt natürlich genauso für eine virtualisierte Umgebung, in der sich MailCleaner ebenfalls sehr wohl fühlt. Als leistungsfähiger Mailserver (MTA) werkelt auf MailCleaner „Exim" und das Projekt „MailScanner" sorgt in Kombination mit den anderen Antispam-Mechanismen für eine sorgfältige Erkennung von Spam und Viren. Die Verwaltung des Systems erledigt der Administrator über ein komfortables Web-Frontend.

Die Arbeitsweise von MailCleaner

MailCleaner arbeitet als klassisches SMTP-Gateway und erwartet die Einlieferung von E-Mails über das SMTP-Protokoll – ein Empfang von Nachrichten über POP3 oder IMAP ist prinzipiell nicht vorgesehen. Typischerweise nimmt MailCleaner E-Mails also direkt aus dem Internet entgegen, was eine feste IP-Adresse für den MX-Record erfordert. Die meisten Privatanwender dürften allerdings nur über eine dynamische IP-Adresse verfügen. Im Kasten „Privates Mail-Gateway mit fetchmail" verraten wir Ihnen darum, wie Sie das Programm „fetchmail" unter MailCleaner installieren und einrichten. fetchmail kümmert sich dann um den Abruf Ihrer E-Mails per POP3- oder IMAP-Protokoll beim Provider und übergibt diese dann zur weiteren Verarbeitung an MailCleaner.

Spam unter Arrest

MailCleaner kann als Spam identifizierte E-Mails entweder mit einem Vermerk in der Betreffzeile an den eigentlichen Mailserver weiterleiten oder diese in speziellen Quarantäneverzeichnissen auf der MailCleaner-Appliance verwalten. Zwar erlauben beide Verfahren dem Benutzer, eventuell irrtümlich als Spam eingestufte E-Mails – so genannte false positives – selbst freizugeben, die Verwaltung des Spams auf der Appliance ist aber der wesentlich elegantere Ansatz. MailCleaner lässt sich so einstellen, dass es dem Benutzer täglich, wöchentlich oder monatlich einen „Spam-Report" per E-Mail schickt, so wie das von zahlreichen Mail-Anbietern bekannt ist. Der Spam-Report enthält einen Überblick über die in Quarantäne aufgelaufenen E-Mails und erlaubt so eine rasche Kontrolle der Quarantäne auf false positives. Zur Freigabe von E-Mails oder zum Löschen des aufgelaufenen Spams loggt sich der User dann über den im Report enthaltenen Link im Benutzerportal auf der MailCleaner-Appliance ein.

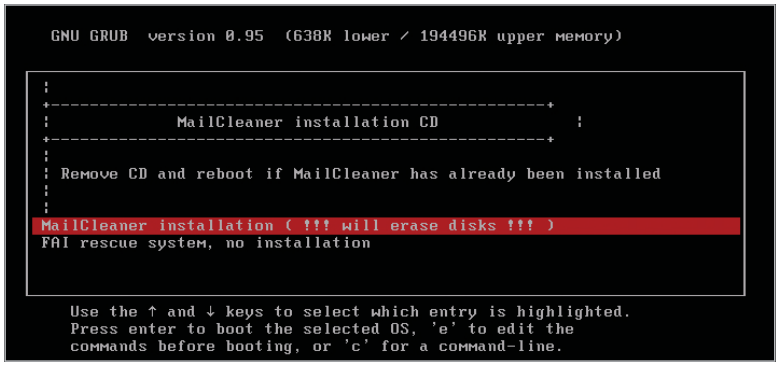
Installation

Sie finden ein ISO-Image von MailCleaner auf unserer Heft-DVD oder Sie laden sich zur Installation die jeweils neueste Version von Webcode*: LIBFAZ herunter, aktuell „mailcleaner_2006 090101.iso". Brennen Sie dieses ISO-Image auf einen CD-Rohling. Die Installation gliedert sich in die folgenden drei Phasen: Installation von Debian GNU/Linux, Installation der MailCleaner-Software und Konfiguration.

MailCleaner-Software installieren

Loggen Sie sich auf der Konsole mit dem Benutzer „root" und dem Passwort „def" ein und starten Sie die Installation der MailCleaner-Software mit dem Befehl:

```
/root/mailcleaner_install.sh
```



Starten Sie Ihren MailCleaner-Rechner von der CD und wählen Sie im Bootmenü den Eintrag „MailCleaner installation" (links)

Beachten Sie, dass evtl. auf der Platte vorhandene Daten während der Installation von MailCleaner unwiederbringlich gelöscht werden (rechts)

Nachfolgend müssen Sie einige Fragen zur gewünschten Konfiguration beantworten. Übernehmen Sie dabei die vorgeschlagenen Pfade und verwenden Sie die HostID 1 für die hier verwendete „Ein-Server"-Installation. Wählen Sie einen passenden Host- und Domainnamen, vergeben Sie ein Passwort für den Admin-Benutzer und verneinen Sie die Frage, ob MailCleaner mit einer interaktiven Installation fortgesetzt werden soll. Je nach Leistungsfähigkeit Ihrer Maschine ist die Installation nach etwa fünf Minuten abgeschlossen. Möchten Sie den Installationsverlauf verfolgen, loggen Sie sich mit „Alt + F2" einfach auf einer zweiten Konsole ein und lassen sich den Fortschritt dort mit dem Befehl

```
tail -f /tmp/mailcleaner_install.log
```

anzeigen. Nach Abschluss der Installation können Sie mit Hilfe des Befehls

```
/root/bin/ip_configurator
```

die IP-Adresse, Default-Gateway und DNS-Server Ihrer MailCleaner-Appliance ändern. Per Default ist das System unter der IP-Adresse 192.168.1.101 im Netzwerk erreichbar. Um ein deutsches Keyboard-Layout zu laden, verwenden Sie den Befehl:

```
loadkeys /usr/share/keymaps/i386/qwertz
/de.kmap.gz
```

Damit MailCleaner beim Systemstart automatisch das richtige Keyboard lädt, kopieren Sie die entsprechende kmap-Datei an die richtige Stelle

```
cp /usr/share/keymaps/i386/qwertz
/de.kmap.gz /etc/console/boottime.kmap.gz
```

Abschließend führen Sie einen Reboot durch.

Login & Basis-Konfiguration

Rufen Sie nun im Webbrowser die URL https://192.168.1.101/admin auf und loggen Sie sich dort mit dem Benutzer „admin" und dem während der Installation vergebenen Passwort ein. Prüfen Sie zunächst die Grundeinstellungen für das Netzwerk, den Zeitserver und den Admin-Benutzer unter „Configuration / Base system". Weiterhin sollten Sie unter „Configuration / SMTP" einstellen, aus welchen IP-Netzen MailCleaner Mails relayen darf. Bei Bedarf schränken Sie weiterhin unter „Configuration / External Access" ein, aus welchen Netzen ein Zugriff auf das Admin-Frontend und per SSH erlaubt ist. In diesem Dialog können Sie auch festlegen, ob MailCleaner über das SMTP-Protokoll von überall (0.0.0.0/0) oder nur aus bestimmten Netzen erreichbar ist. Ist das erledigt, legen Sie als nächstes Ihre Mail-Domain(s) unter „Domains / View and manage" an, indem Sie dort auf das Pluszeichen klicken. Tragen Sie mindestens den Domainnamen sowie unter „Destination Server" die IP-Adresse Ihres internen Mailservers ein. Wählen Sie dann unter „Action on spam" aus der Liste aus, ob als Spam erkannte E-Mails nur im Betreff markiert (tag), komplett verworfen (drop) oder in die Benutzerquarantäne auf der MailCleaner-Appliance verschoben werden sollen (quarantine). Entscheiden Sie sich für die Benutzerquarantäne, wählen Sie im Bereich „User authentication" aus, wie sich die Benutzer authentifizieren sollen. In unserem Fall werden wir die Benutzer auf der MailCleaner-Appliance anlegen und entscheiden uns daher für „con-

Kurz erklärt – MX-Record

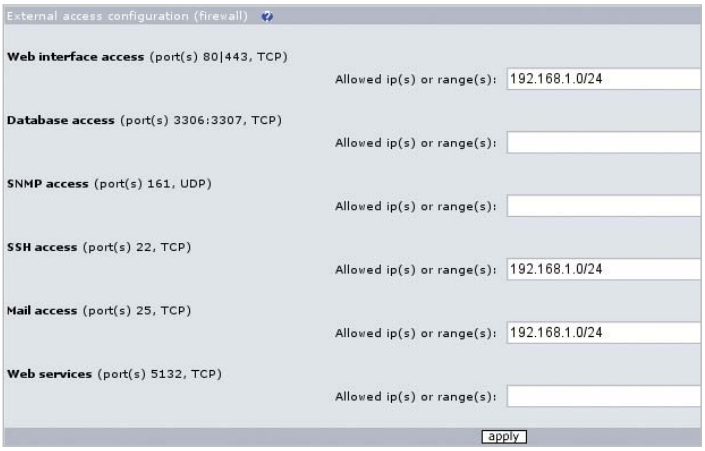
Der MX- (= Mail Exchange) Record beschreibt, welcher Mailserver für den Empfang von E-Mails für eine bestimmte Internet-Domain zuständig ist. Prinzipiell können für eine Internet-Domain auch mehrere Mailserver einen MX-Eintrag erhalten, z. B. um den SMTP-Verkehr auf mehrere Mailserver zu verteilen oder um Backup-Szenarien bei Ausfall eines Mailservers zu schaffen. Die Reihenfolge ihrer Zuständigkeit wird dabei über einen numerischen Wert zur Priorisierung festgelegt. Den MX-Record für Domains können Sie leicht in der Shell abfragen. So liefert der Befehl:

```
dig mx databecker.de
folgendes Ergebnis (Ausgabe gekürzt):
databecker.de. 86400 IN MX 60 mx2.mail1.databecker.de.
databecker.de. 86400 IN MX 60 mx1.mail1.databecker.de.
databecker.de. 86400 IN MX 40 mail2.databecker.de.
databecker.de. 86400 IN MX 50 pcpraxis.databecker.de.
databecker.de. 86400 IN MX 30 mail1.databecker.de.
```

Der Mailserver mit dem niedrigsten numerischen Wert (hier 30) ist der Mailserver mit der höchsten Priorität. Senden Sie eine E-Mail an einen Empfänger in der Domain databecker.de, versucht Ihr Mailserver also zunächst mail1.databecker.de zu erreichen. Ist dieser nicht verfügbar, versucht Ihr Mailserver der Reihe nach mail2.databecker.de, pcpraxis.databecker.de und zuletzt mx1 bzw. mx2.databecker.de zu erreichen.

Zusätzliche Admins einrichten

Sie können neben Quarantäne-Benutzern auch zusätzliche Benutzer mit granular abgestuften administrativen Rechten anlegen. Sie finden den entsprechenden Dialog unter „Configuration / Administration". Für jeden Administrator können Sie individuell festlegen, welche Domains dieser verwalten darf, ob er Zugriff auf die System- und Benutzerkonfiguration hat oder nur Statistiken einsehen darf.



Für die Installation der MailCleaner-Software müssen Sie nur wenige Fragen beantworten. Die weiterführende Konfiguration nehmen Sie über ein komfortables Web-Frontend vor (links)

Unter „External Access" legen Sie fest, aus welchen Netzen MailCleaner per Webschnittstelle und SSH administriert werden darf. Hier lässt sich auch einschränken, aus welchen Netzwerken MailCleaner überhaupt Nachrichten per SMTP entgegennimmt (rechts)

nector / local". MailCleaner bietet mit den beiden Optionen „Enable SMTP callout" und „Enable LDAP/AD callout" an, entweder auf dem internen SMTP-Server oder in einem Verzeichnisdienst wie zum Beispiel einem LDAP-Server oder einem ActiveDirectory nachzusehen, ob der E-Mail-Empfänger tatsächlich existiert. Existiert der Benutzer nicht, lehnt MailCleaner die Zustellung der betroffenen E-Mail ab. Das funktioniert nur, wenn Sie MailCleaner als echtes SMTP-Gateway einsetzen. Rufen Sie Ihre E-Mails per fetchmail ab, deaktivieren Sie diesen Mechanismus. Das gilt ebenso für die Aktion „Enable greylisting", denn Greylisting blockiert den Empfang von E-Mails mit bisher unbekannten Absender-Empfänger-Mailserver-Kombinationen und nimmt E-Mails erst nach einem zweiten, RFC-konformen Zustellversuch entgegen. Dem Greylisting-Prinzip liegt die Annahme zugrunde, dass Spamschleudern immer nur einen Zustellversuch unternehmen. Die Voreinstellungen im Bereich „Filtering" können Sie einfach übernehmen. Bei den „Preferences" legen Sie die Sprache für die Login-Seite des User-Frontends fest und in welchem Format (html oder plain text) bzw. in welcher Frequenz (täglich, wöchentlich, monatlich) MailCleaner Spam-Reports an Ihre Benutzer verschicken soll.

Quarantäne-User anlegen

Da jeder Benutzer seine persönliche Spam-Quarantäne erhält, die er später über ein Web-Frontend einsehen kann, müssen Sie unter „users / Manage by Users" nun natürlich noch die gewünschten Benutzerkonten anlegen. Tippen Sie den Benutzernamen ein und klicken Sie auf den schwarzen Pfeil. Daraufhin öffnet sich ein weiterer Dialog, in dem Sie die Sprache, das Passwort, den Realnamen und die E-Mail-Adresse(n) des neuen Users festlegen können. Klicken Sie zum Speichern auf den Button „apply".

Contentfilter aktivieren

Neben dem Schutz vor Spam und Viren liefert MailCleaner auch einen leistungsfähigen Contentfilter mit. Dieser analysiert eingehende E-Mails auf potenziell gefährlichen Content. Die Konfiguration des Contentfilters nehmen Sie im Dialog „Configuration / Dangerous Content" vor. Der HTML-Content Checker untersucht HTML-Mails auf gefährlichen Code wie iFrames, Web-Bugs und Script Tags und kann diese

Flickenteppich

Wie bei jedem anderen System müssen auch in MailCleaner ab und an Patches eingespielt werden. Diese beheben in der Regel Fehler in der Software und rüsten zusätzliche Funktionen nach. Leider ist der Patch-Mechanismus in der Open-Source-Version derzeit nicht sonderlich elegant gelöst – Patches müssen daher manuell heruntergeladen und chronologisch „von Hand" installiert werden. Um die Patches herunterzuladen, wechseln Sie in Ihr MailCleaner-Installationsverzeichnis, normalerweise /usr/mailcleaner, und geben den Befehl

```
cvs update -dP updates
```

ein. Kurze Zeit später werden die heruntergeladenen Patches aufgelistet:

```
2006090401
2006100201
2006111701
2007012801
2007080901
2009012201
```

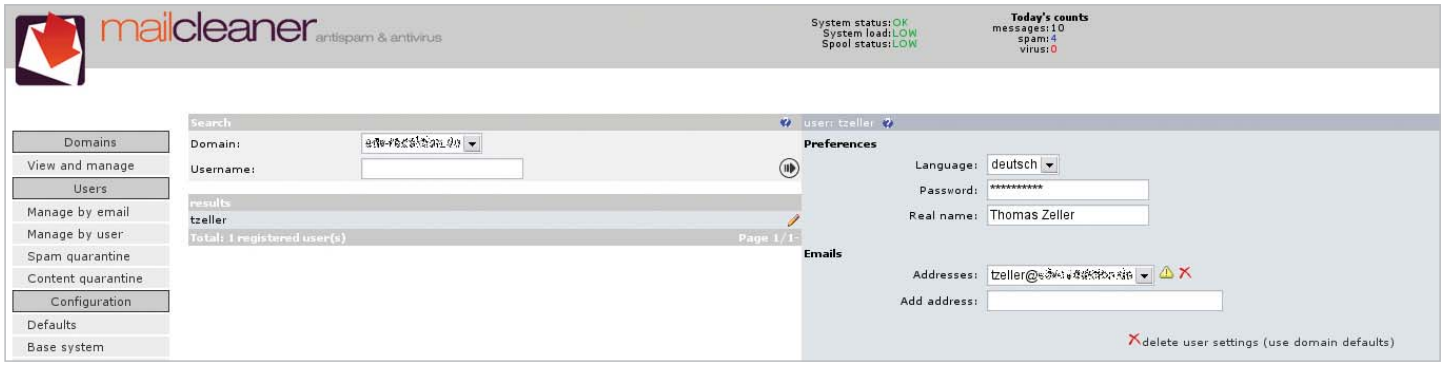
Spielen Sie diese nun der Reihe nach mit folgendem Befehl in Ihr System ein:

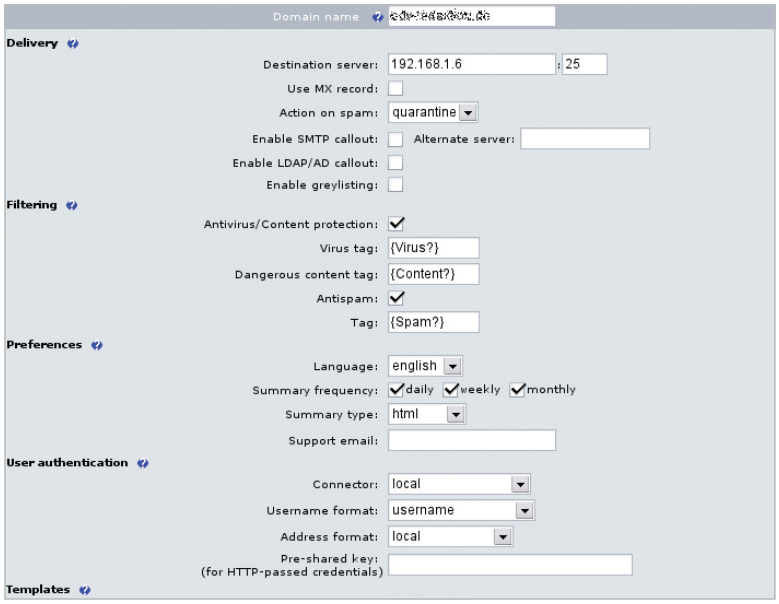
```
bin/apply_update.sh <PATCHNUMMER>
```

Während die ersten fünf Patches in wenigen Sekunden installiert sind, benötigt das Einspielen des neuesten Patches „2009012201" bis zu 30 Minuten! Haben Sie also etwas Geduld und brechen Sie die Installation keinesfalls vorzeitig ab.

Im Namen des Gesetzes

Beim Einsatz eines Spamfilters in Unternehmen ist Vorsicht geboten. Denn ist die private Nutzung des geschäftlichen E-Mail-Accounts erlaubt, gilt der Arbeitgeber als Telekommunikationsanbieter im Sinne des Telekommunikationsgesetzes und übernimmt damit faktisch die Rolle eines Internet-Providers für seine Mitarbeiter. In diesem Fall dürfen E-Mails nicht auf unerwünschte Inhalte gefiltert und schon gar nicht unterdrückt werden, es sei denn, der Benutzer hat diesem Verfahren explizit zugestimmt. Unternehmen sind daher gut beraten, einen Spamfilter einzusetzen, der als Spam erkannte E-Mails markiert – z. B. indem der Begriff ***SPAM*** in der Betreffzeile hinzugefügt wird -, um diese dann per Filterfunktion am Mail-Client in einen Spam-Ordner zu verfrachten. Wesentlich eleganter ist es allerdings, als Spam erkannte E-Mails in einem Quarantäne-Bereich zu sammeln und jedem Benutzer Zugriff auf seine individuelle Quarantäne zu gewähren. Auf diese Weise kann sich der Benutzer irrtümlich als Spam erkannte E-Mails selbst freigeben und die gesetzlichen Vorgaben zur Wahrung des E-Mail-Verkehrs werden erfüllt. MailCleaner beherrscht beide Verfahren und eignet sich daher auch bestens für den Unternehmenseinsatz.





MaiCleaner kann mehrere Domains verwalten und diesen unterschiedliche Mailserver zuweisen. Auf diese Weise eignet sich MailCleaner auch als Gateway für Hostingfarmen (links)

Jeder User erhält auf der MailCleaner-Appliance sein eigenes Quarantäne-Verzeichnis. Auf diese Weise kann sich der Benutzer irrtümlich als Spam erkannte E-Mails selbständig freigeben, ohne dafür einen Administrator zu bemühen (oben)

Elemente entweder durchlassen, blockieren oder deaktivieren. Die „Message format checks“ erlauben darüber hinaus passwortgeschützte Archive oder verschlüsselte Nachrichten zu blockieren.

Noch einen Schritt weiter gehen die „Attachment checks“, mit deren Hilfe sich E-Mails mit bestimmten Dateianhängen blockieren lassen. Leider ist die Liste der vorhandenen Dateien statisch und lässt sich daher nicht individuell erweitern. Immerhin werden derzeit aber bereits die folgenden Dateitypen erkannt:

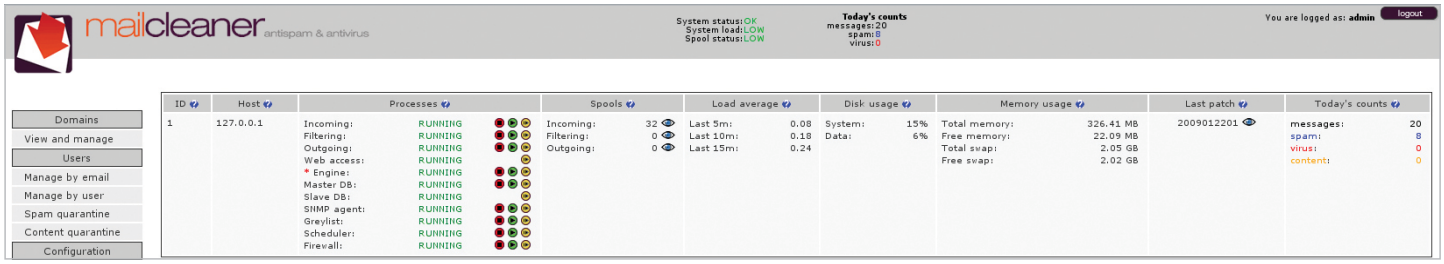
- text (Textfiles)
- script (Skripte)
- archive (Kompressionsprogramme)
- self-extract (Selbstextrahierende Archive)
- ELF + executable (Programme)
- MPEG, AVI, MNG und QuickTime (diverse Film-Formate)
- Registry (Windows Registry Keys)

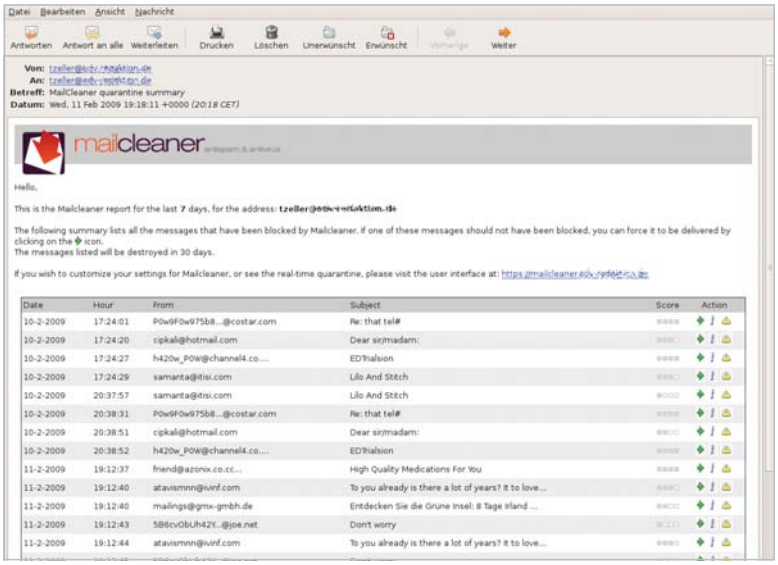
Fette Beute

Nach Abschluss der Konfiguration von MailCleaner können Sie die Funktionen im Live-Betrieb testen. Unabhängig davon, ob Sie MailCleaner als SMTP-Gateway oder mit Unterstützung von fetchmail betreiben, können Sie MailCleaner unter „Monitoring / Status“ jederzeit bei der Arbeit zuschauen. In der Tabelle finden Sie ganz rechts die Anzahl der heute insgesamt verarbeiteten Nachrichten, unterteilt in Spam- und Viren-

Mit Hilfe des Contentfilters kann MailCleaner E-Mails mit gefährlichen Attachments stoppen, den Empfang passwortgeschützter oder verschlüsselter Archive verhindern, bestimmte Datei-Extensions blocken und vieles mehr (links)

MailCleaner verarbeitet eingehende E-Mails in drei Spools: Der „Incoming-Spool“ listet eingehende Nachrichten auf und reicht diese dann an den „Filtering-Spool“ weiter. Die gefilterten Nachrichten wandern dann weiter an den „Outgoing-Spool“. Auf diese Weise können Sie den vollständigen Prozess der Mailbearbeitung von MailCleaner jederzeit mitverfolgen (unten)





Per MRTG erzeugte Grafiken versorgen den Administrator mit statistischen Informationen zur Ressourcenauslastung der MailCleaner-Appliance (links)

MailCleaner erzeugt auf Wunsch tägliche, wöchentliche oder monatliche Spam-Reports an die Benutzer. Über den im Report enthaltenen Link können sich Benutzer direkt in ihre Spam-Quarantäne einloggen und dort Nachrichten selbständig freigeben oder löschen (rechts)

mails, sowie solche, die aufgrund einer Contentfilterregel blockiert wurden. Den aktuellen Bearbeitungszustand spiegelt die Spalte „Spools“ wieder. Unter „Incoming“ sehen Sie wieder die Anzahl der eingegangenen Nachrichten insgesamt, unter „Filtering“ angezeigte Nachrichten werden gerade von den verschiedenen Filter-Engines untersucht und der „Outgoing“-Spool informiert darüber, wie viele Nachrichten gerade zu Ihrem Mailserver unterwegs sind. Ein Klick auf das „Auge“-Icon des entsprechenden Spools öffnet ein Pop-up-Fenster, in dem die derzeit in Bearbeitung befindlichen Mails aufgelistet werden. Je mehr E-Mails pro Stunde MailCleaner verarbeiten muss, desto eher sollten Sie ein wachsames Auge auf die Ressourcen haben, die MailCleaner zur Verfügung stehen. Grafisch aufbereitete, statistische Informationen wie die Auslastung von Prozessor, Arbeitsspeicher und Festplatte sowie zur Netzwerk- und Systemlast durch MailCleaner erhalten Sie unter „Monitoring / Statistics“.

Besuch im Gefängnis

Als Administrator haben Sie selbstverständlich Zugriff auf sämtliche Quarantänen. Klicken Sie auf „Users / Spam quarantine“ und tragen Sie in das Suchfeld den Namen eines Benutzers ein – sofort sehen Sie alle Nachrichten in dessen Quarantäne. Alternativ können Sie die Quarantänen auch durch die Eingabe von Suchstrings im From-Feld oder im Betreff durchsuchen. Wie erhalten aber die Benutzer Zugriff auf ihre Quarantäne-Verzeichnisse? Haben Sie beim Anlegen des Benutzers den Versand eines Spam-Reports veranlasst, klickt der Benutzer auf den entsprechenden Link in der Report-E-Mail. Das User-Portal ist unter der URL http://HOSTNAME.DOMAIN erreichbar. Haben Sie während der Installation den Hostnamen „mailcleaner“ und die Domain „user.org“ angegeben, erreichen Sie das User-Portal unter „http://mailcleaner.user.org“. Für den Zugriff auf das Quarantäne-Verzeichnis muss sich

Privates Mail-Gateway mit fetchmail

MailCleaner basiert auf Debian GNU/Linux 3.1. Prinzipiell ist es daher kein Problem, zusätzliche Pakete auf die MailCleaner-Appliance zu packen. Richten Sie zunächst die Debian-Paketverwaltung mit Hilfe des Befehls

```
apt-setup
```

ein. Wählen Sie als Repository einen HTTP- oder FTP-Server in Ihrer Nähe aus, aktualisieren Sie die Paketliste mit dem Befehl

```
apt-get update
```

und installieren Sie fetchmail durch Eingabe von

```
apt-get install fetchmail
```

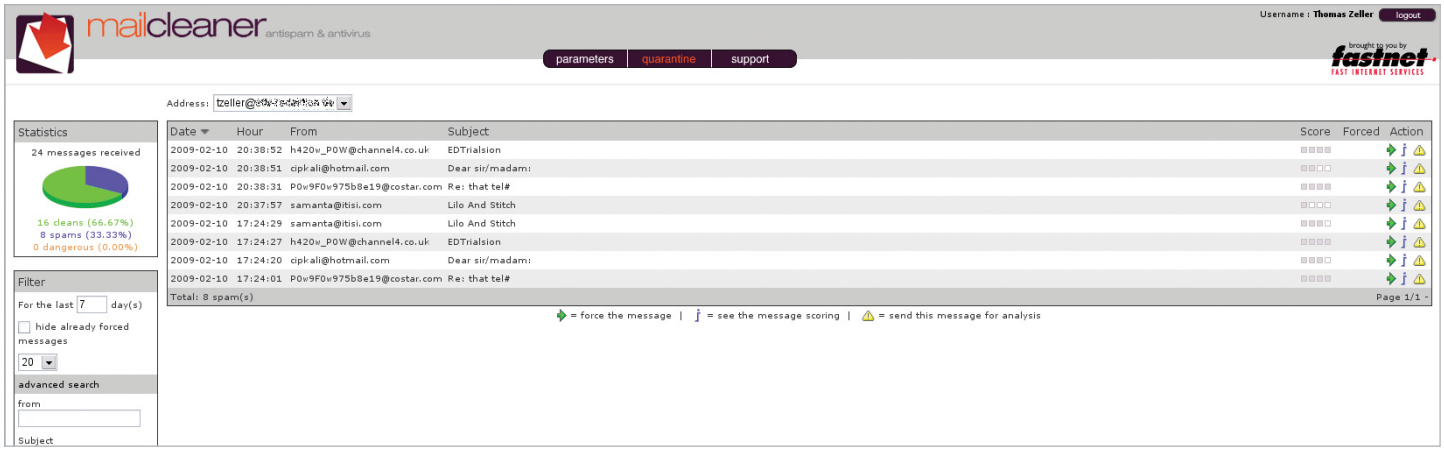
Legen Sie dann mit Hilfe des Befehls „adduser“ einen Benutzer auf dem System an, unter dessen Kennung später Ihre POP3-Konten abgerufen werden. Im Homeverzeichnis des neuen Benutzers erstellen Sie dann die Datei „.fetchmailrc“ (achten Sie auf den führenden Punkt). Die Syntax der Datei ist einfach. So werden mit dem Eintrag:

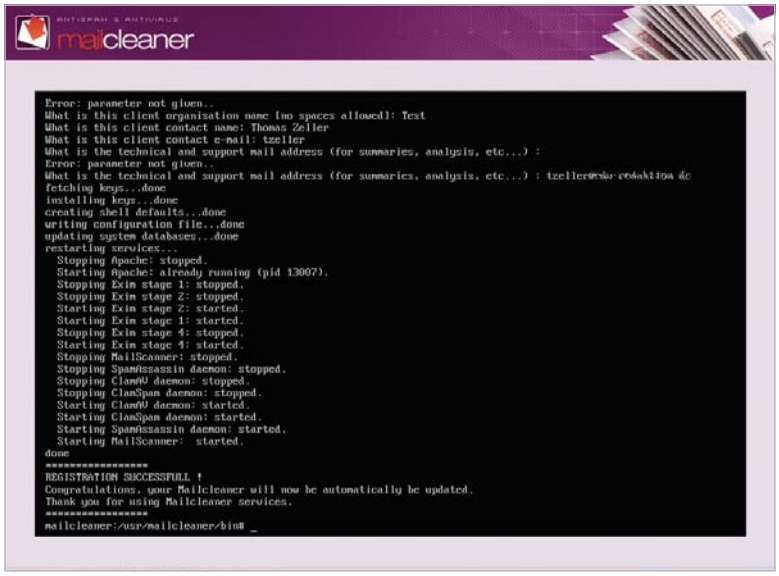
```
poll pop.provider.de with protocol pop3
user Asterix there is Obelix@lokale-Domain-Ihres-Mailcleaner-Rechners
here
```

E-Mails für den Benutzer Asterix beim Mailserver pop.provider.de abgerufen und an den lokalen Benutzer Obelix weitergeleitet. Wichtig ist, dass Sie für den lokalen Benutzer eine der Domains verwenden, die Sie bei der Konfiguration von MailCleaner verwendet haben – MailCleaner kennt damit den zuständigen Mailserver (IP-Adresse) in Ihrem Netzwerk und kümmert sich um die Zustellung der „sauberen“ E-Mails. Zum Abrufen der E-Mails loggen Sie sich nun als „root“ per SSH in Ihre MailCleaner-Appliance ein, wechseln mit „su – <Benutzer>“ die Benutzerkennung zu dem soeben angelegten Benutzer und starten den Abruf Ihrer E-Mails durch den Befehl:

```
fetchmail -v
```

Sie können dann in der Konsole mitverfolgen, wie fetchmail die Nachrichten vom Server Ihres Providers abruft. Klappt alles wie gewünscht, fügen Sie den Aufruf von fetchmail einfach Ihrer Crontab hinzu, damit MailCleaner sich künftig automatisch um den Abruf Ihrer E-Mails kümmert.





Die Benutzer-Quarantäne ist auch für wenig versierte Anwender intuitiv bedienbar. Hier können Benutzer die Quarantäne bei Bedarf auch selbständig abschalten (oben)

In der kommerziellen Version von MailCleaner muss sich der Administrator nicht selbst um das Einspielen von Updates und Optimierungen kümmern. Nach erfolgreicher Registrierung der Appliance beim Schweizer Hersteller Fastnet versorgt sich das System selbständig mit den erforderlichen Updates (links)

der Benutzer mit jenen Daten authentifizieren, die der Administrator beim Anlegen des Benutzers vergeben hat. Nach erfolgreichem Login zeigt MailCleaner per Default alle in der Quarantäne aufgelaufenen Nachrichten der letzten sieben Tage an. Rechts neben den Nachrichten finden sich drei Symbole: Mit einem Klick auf den grünen Pfeil kann sich der Benutzer Nachrichten in seinen Mail-Account zustellen lassen. Ein Klick auf das blaue, stilisierte „i“ öffnet ein Pop-up-Fenster, in dem Sie haarklein nachvollziehen können, warum eine E-Mail in der Quarantäne gelandet ist. Das gelbe Symbol mit dem Ausrufezeichen schließlich erlaubt das Weiterleiten einer Nachricht an den Administrator von MailCleaner zum Zwecke einer genaueren Analyse. Damit das funktioniert, müssen Sie die E-Mail-Adresse des Administrators in den Einstellungen zum Domain-Namen unter „Support email“ angeben.

MailCleaner kommerziell

Die kommerzielle Variante von MailCleaner bringt für die Installation einen textbasierten Assistenten mit, der zunächst alle relevanten Informationen an der Konsole abfragt und das System dann vollautomatisch einrichtet. Weiterhin kann nur die kommerzielle Version Updates vom Fastnet-Update-Server beziehen, um auf diese Weise stets gegen die neuesten Viren und Tricks der Spammer gewappnet zu sein. Zur Einrichtung der Updates ist zunächst eine Registrierung mit den Zugangsdaten erforderlich, die Sie beim Kauf der Software erhalten haben. Führen Sie dann das Skript

```
/usr/mailcleaner/bin/register_mailcleaner.sh
```

aus und tragen Sie Ihre Zugangsdaten entsprechend ein. Hat alles geklappt, beendet sich das Skript mit der Meldung „REGISTRATION SUCCESSFULL“. MailCleaner prüft dann automatisch alle 15 Minuten, ob neue Antispam- und Antivirus-Updates für Ihr System bereitstehen und lädt diese herunter.

Profiwerkzeug gegen Spam

Die Antispam-Software MailCleaner ist bereits in der vorliegenden Open-Source-Version bestens für den Antispam- und Antivirus-Einsatz im privaten Bereich oder auch in kleineren Unternehmen geeignet, auch wenn die freie Variante inzwischen das Ende des Produktlebenszyklus erreicht hat. Major-Updates wird es für die vorliegende Version daher nicht mehr geben. Die kommerzielle Version skaliert nach Angaben des Herstellers Fastnet auch für tausende von Benutzern noch hervorragend und weitere Entwicklungen für die kommerzielle Version kommen auch der Open-Source-Version zugute. Fastnet hat bereits für den Herbst 2009 eine komplett neue Open-Source-Version von MailCleaner in Aussicht gestellt, die sich im Look & Feel an der kommerziellen Variante orientiert – wir dürfen gespannt sein.

Preise der kommerziellen MailCleaner-Version

Die kommerzielle Version von MailCleaner schlägt im ersten Jahr mit Euro 1.200,00 für 245 Mailboxen zu Buche. Ab dem zweiten Jahr fallen weitere Euro 853,66 jährlich für die Softwarepflege an. Bildungseinrichtungen erhalten auf Anfrage Sonderkonditionen, das Unternehmen „Fastnet“ bietet MailCleaner alternativ auch als Hosted Service an. Für Euro 300,00 pro Jahr und Domain lassen sich so bis zu 20.000 E-Mails pro Monat im externen Rechenzentrum filtern. Die Preisliste ist öffentlich und steht auf der MailCleaner-Website zur Verfügung: Webcode*: LI4D4K. Die Preise für die Hosted Services von Fastnet finden Sie unter: Webcode*: LIESSM.