Server-Kammerjäger

Ein Großteil aller Computerschädlinge wird per Mail verbreitet. Aber auch Dateiserver sind beliebte Virenschleudern. Höchste Zeit also, die eigenen Server gegen Viren zu schützen. Linux Professionell zeigt, wie Postfix, Amavis, Dazuko und ClamAV den digitalen Plagegeistern den Garaus machen.

ACHIM WAGENKNECHT

Die meisten Provider filtern Viren und ähnliche Schädlinge zuverlässig aus dem E-Mail-Traffic, so dass es der gefährliche Code gar nicht mehr auf das System des Anwenders schafft. Um nicht unangenehm als Virenschleuder aufzufallen, sollten Sie die eigenen Mail- und Dateiserver ebenfalls gegen Viren schützen.

Wir zeigen Ihnen, wie Sie den Mail-Server Postfix mit dem Open-Source-Antivirenprogramm ClamAV und der Schnittstelle Amavis schützen. Anschließend erfahren Sie, wie Sie von Ihnen administrierte Samba- und Netatalk-Server mit ClamAV und dem Kernel-Modul Dazuko sichern.

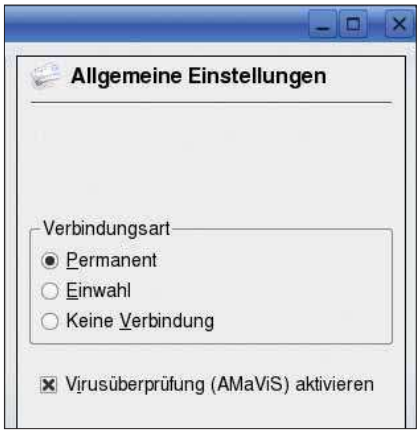
Mail-Server absichern

Wer eine aktuelle Suse-Version im Zusammenspiel mit Postfix einsetzt, hat scheinbar leichtes Spiel im Kampf gegen E-Mail-Viren: Der Administrator aktiviert einfach im Yast-Modul *Netzwerkdienste/Mail Transfer Agent* die Option *Virusüberprüfung* und wähnt sich auf der sicheren Seite. Andere Distributionen bieten ähnlich komfortable Einstellungen, die die Sicherheit erhöhen.

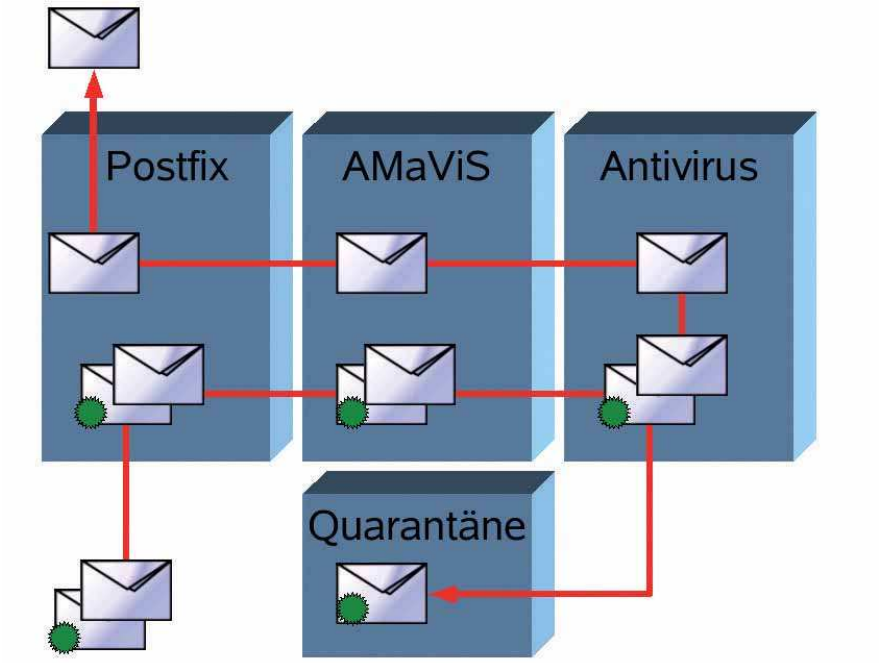
Wer sich darauf aber verlässt, kann eine herbe Enttäuschung erleben, da das hier aktivierte Amavis keine Antiviren-Software, sondern lediglich eine Schnittstelle ist.

Sicherheitsstatus ermitteln

Wollen Sie herausfinden, ob Ihr Mail-Server wirklich gegen Viren geschützt ist, müssen Sie eine Testumgebung aufbauen und Viren an sich selbst verschicken. Im Linux-Professionell-Labor haben die Tester das mit zwei Linux-Rechnern durchgespielt. Die Rechner heißen *links.work* und *rechts.home*. Auf beiden Systemen wird der Benutzer *test* eingerichtet. Damit die Mails von *work* nach *home* gesendet werden können, muss die IP-Adresse des *home*-Mail-Servers im *work*-MTA als *Ausgehender Mail-Server* eingetragen sein. Dann wird der *home*-MTA in Yast so konfiguriert, dass er entfernte SMTP-Verbindungen akzeptiert.



Irreführend: Amavis ist keine Software zur Abwehr von Viren



Virenfreie Mails: Die Schnittstelle Amavis reicht die Mails vom Mail-Server Postfix an das Antivirenprogramm weiter und gibt sie gefiltert zurück

Nun können Sie gefahrlos virenverseuchte Mails von *work* an die Adresse *test@rechts.home* senden und in Eigenregie ermitteln, wie es um die Sicherheit des von Ihnen betriebenen E-Mail-Servers bestellt ist.

Nur ein Placeboeffekt?

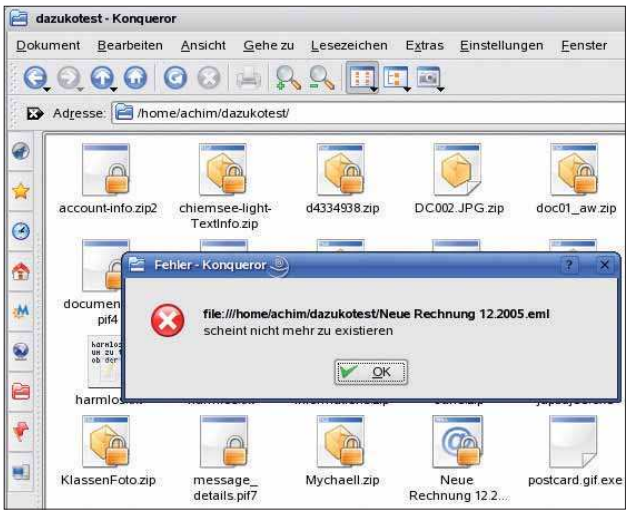
Ist Amavis deaktiviert, kommen erwartungsgemäß alle Viren an. Das gleiche Bild zeigt sich aber auch dann, als die Tester Amavis aktivieren: Es werden immer noch alle Schädlinge ausgeliefert. Der Virenschutz nur ein Placebo? Nicht ganz. Es zeigt sich, dass die Einstellung in Yast irreführend ist. Aktiviert wird hier nämlich nur die Antiviren-Schnittstelle Amavis. Und obwohl Amavis für »A Mail Virus Scanner« steht, scannt das Programm nicht selbst.

Die Anwendung stellt lediglich einen Systemdaemon bereit, der den Datenfluss zwischen Mail Transfer Agent und Content-Filtern regelt. Ob an diese Schnittstelle auch wirklich ein Antivirenprogramm angeschlossen ist, verrät Yast nicht. Wer aber die Option zum ersten Mal aktiviert und dabei die Systemmeldungen im Auge behält, sieht, dass das Open-Source-Antivirenprogramm ClamAV installiert wird.

ClamAV hilft weiter

Nur wird – wie ein Blick in die Prozesstabelle zeigt – der Systemdaemon von ClamAV namens *clamd* nicht von Yast gestartet. Um den Virenschutz wirklich zu aktivieren, ist also Handarbeit angesagt.

Es gilt, den Systemdaemon von ClamAV zu starten und mit dem Mail-Server Postfix zu verbinden. Und damit ClamAV permanent gegen Viren schützt, muss das Tool regelmäßig aktualisiert werden. Dazu dient das Programm *fresh clam*, das per cronjob



Erwischt: Mit Hilfe des Kernel-Moduls Dazuko blockiert ClamAV infizierte Dateien auf Samba-Servern

mindestens einmal täglich ausgeführt werden sollte, besser noch einmal stündlich. Auch sollten Sie das Tool gleich nach der Einrichtung des Virenschutzes per Hand aufrufen. Praktische Funktion: Die Routine stellt fest, ob die Virensignaturen von ClamAV noch aktuell sind, ohne die Download-Server abfragen zu müssen. Dies ist möglich, da die Entwickler den aktuellen Status der Signaturen direkt im DNS hinterlegen.

Zusammenspiel erzwingen

Kommen trotz laufendem und aktualisiertem ClamAV noch Viren an, dann gilt es, das Zusammenspiel von Postfix, Amavis und ClamAV zu überprüfen. Neben ClamAV haben die Tester das übrigens auch mit zwei kommerziellen Antivirenprodukten getestet: Antivir von Avira und AVG von Grisoft. Die Verbindung vom Antivirenprodukt zu Amavis ist in allen drei Fällen relativ einfach herzustellen. Antivir wird im Test sogar automatisch eingebunden. Allerdings wird Antivir für jede einzelne Mail erneut gestartet, was sich als große Systembremse herausstellt. Wird der Aufruf von Antivir jedoch in der Datei */etc/amavisd.conf* auskommentiert, erhöht sich die Geschwindigkeit des E-Mail-Versands um den Faktor fünf.

Wesentlich komplexer ist es, Postfix so einzurichten, dass das Tool reibungslos mit Amavis zusammenarbeitet.

Verschlungene Pfade

Aber wie arbeitet der digitale Kammerjäger überhaupt? In der Standard-Konfiguration sendet Postfix ungeprüfte Mails zunächst an den Port *10024* auf *localhost*. Dort nimmt Amavis sie in Empfang und leitet sie an das angeschlossene Antivirenprogramm weiter. ClamAV nimmt die Mail auf Port *3310* entgegen, AVG auf *5555*. Die voreingestellten Ports lassen sich natürlich in den Konfigurationsdateien ändern. Der Antivirendaemon leitet die Mail dann zurück an Amavis. Von Amavis läuft die Mail wieder an Postfix, diesmal auf Port *10025*. Und zu guter Letzt liefert Postfix die Mail aus. Damit das Procedere schneller vonstatten geht, lassen sich sowohl Amavis als auch die Antiviren-Dämonen in mehreren Instanzen starten, die die Mail-Warteschlange parallel abarbeiten. Voreingestellt sind für den AVG-Daemon zwei Instanzen, für Amavis drei und für ClamAV eine. Um ClamAV mehrfach zu starten, müssen Sie für jede Instanz eine eigene Einstellungs- und Log-Datei einrichten.

Doppelte Virenabwehr

Amavis übernimmt einige Aufgaben, die auf dem Windows-Desktop das Antivirensystem übernehmen muss. Das Tool analysiert Mails, zerlegt Multipart-Nachrichten in ihre Bestandteile, extrahiert Anhänge und entpackt Archive, so dass sich der Virenscanner auf seinen Hauptaufgabenbereich konzentrieren kann. Mails mit verbotenen Headern blockiert Amavis gleich selbst. So werden zum Beispiel typische Windows-Attachments mit vielen Leerzeichen im Dateinamen blockiert. Auch nach dem Scan nimmt Amavis dem Antivirenprogramm Arbeit ab. Die Anwendung entscheidet anhand dessen Konfigurationsdatei, was mit infizierten Mails passieren soll, und löscht oder verschiebt sie in einen Quarantänebereich. Dieser befindet sich in */var/spool/amavis/virusmails/*. Beim Funktionstest sollten alle verdächtigen Elemente in diesem Ordner landen.

Hand in Hand

Im von uns durchgeführten Praxistest ist das zunächst nicht der Fall. Verdächtig erscheint, dass in der Konfigurationsdatei von ClamAV die Option *ScanMail* deaktiviert ist. Diese Funktion hat aber im Zusammenspiel mit Amavis keine Bedeutung, weil das Tool die Dateien ja vorbereitet.

Der Schlüssel ist die Zusammenarbeit zwischen Postfix und Amavis. Diese richten Sie in den beiden Einstellungsdateien von Postfix ein: *master.cf* und *main.cf*. In die Datei *main.cf* tippen Sie folgende Zeile ein, die Amavis als Content-Filter für alle Instanzen von Postfix vordefiniert:

```
content_filter = smtp-amavis:
  [127.0.0.1]:10024
```

Auf die Syntax achten

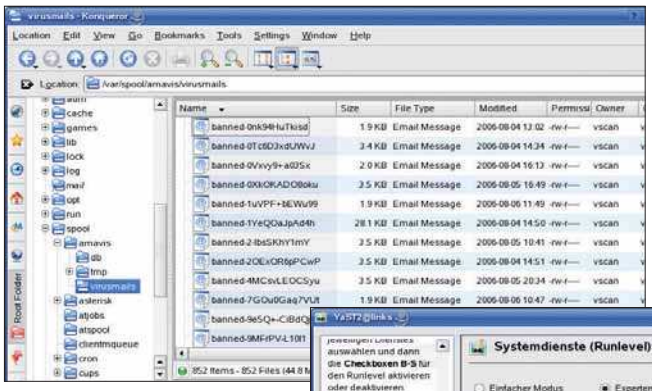
Die Einstellungsdateien von Postfix reagieren empfindlich auf Änderungen. So reicht beispielsweise ein Leerzeichen am Anfang einer Zeile, damit der Befehl falsch ausgewertet wird. Die Suse-Entwickler haben aber noch einen weiteren Stolperstein eingebaut: Die Einstellungen, die das Programm *Suse.Config* erzeugt, werden unkommentiert an das Ende der Datei angefügt.

So kann es in der Praxis leicht passieren, dass nach manuellen Änderungen eine Einstellung zweimal in der Datei vorkommt. Passiert so etwas mit Port-Einstellungen, so startet Postfix möglicherweise nicht mehr, weil es sich zweimal an denselben Port binden soll. Beim zweiten Versuch bricht der Start-

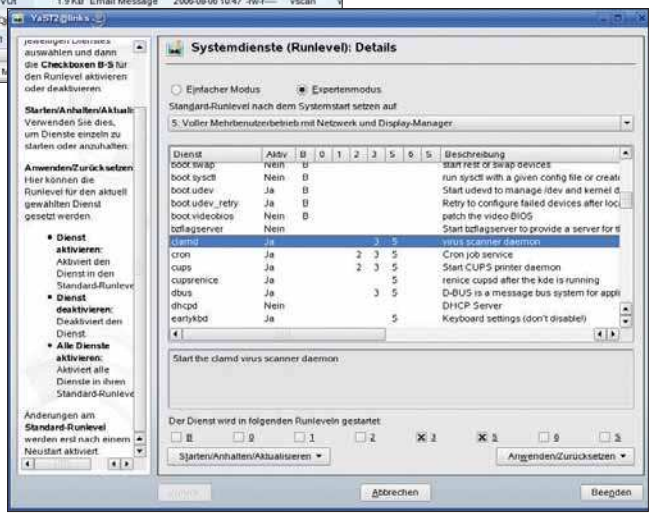
Buchtipp

Wenn Sie das Thema Virenschutz weiter vertiefen wollen, können wir Ihnen dieses Buch besonders ans Herz legen. Es führt in die Grundlagen der Spam- und Virenerkennung ein und vermittelt Abwehrstrategien, die auf der Basis von Postfix, Sendmail und Exim praxisnah umgesetzt werden.

Mit Open Source-Tools Spam & Viren bekämpfen
Autoren: Peter Eisentraut, Alexander Wirt
ISBN: 3-89721-377-X
Verlag: O'Reilly
Preis: 36 Euro
Online: www.oreilly.de/german/freebooks/spamvirger/



Isolierstation: Infizierte Mails landen automatisch im Quarantäne-Ordner



Aktiviert: Damit der Server stets geschützt ist, muss der Antivirus-Daemon in den Startvorgang eingebunden werden, zum Beispiel mit dem Yast-Runlevel-Editor

vorgang dann folgerichtig ab, weil der Port schon belegt ist. Um solchen Problemen vorzubeugen, ist es ratsam, die Konfigurationsdateien immer nur zeilenweise zu editieren und nach jeder Änderung den Mailer mit dem Befehl *postfix reload* neu zu starten. Wie sich die Änderungen auswirken, ist im Verzeichnis */var/log/mail**, vor allem in */var/log/mail.warn* zu erkennen.

Vorsichtig konfigurieren

Mit diesem elementaren Wissen ausgestattet, fügen Sie das folgende Listing in die Datei *master.cf* ein:

```
smtp-amavis unix -  -  y  -  2
  smtp
    -o smtp_data_done_timeout
       =1200
    -o smtp_send_xforward_com
       mand=yes
    -o disable_dns_lookups=yes
    -o max_use=20
```

Der Block definiert den Mail-Transportdienst *smtp-amavis*, der die Verbindung zwischen Postfix und Amavis herstellt. Die eigentliche Ausführung des Transports übernimmt das Postfix-Modul *smtp*. Die Option *unix* sorgt dafür, dass der Dienst nur lokal erreichbar ist. Haben Sie Postfix in einem *chroot*-Bereich abgeschottet, setzen Sie wie in diesem Beispiel die fünfte Option der ersten Zeile auf *y*, ansonsten auf *n*. Die vorletzte Option bestimmt, in wie vielen Instanzen der Prozess höchstens ausgeführt werden darf. In diesem Beispiel sind es zwei. Die Optionen mit *-o* in den folgenden Zeilen optimieren den Ablauf, indem sie Postfix daran hindern, im DNS nachzusehen, weil das bei lokalen Mails schließlich nicht nötig ist.

Weiterführende Optionen

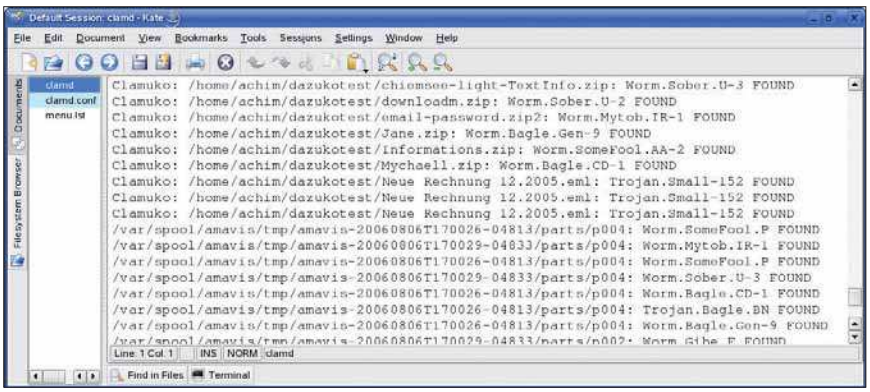
Es folgt ein längerer Block, der den Rückweg der Mails von Amavis nach Postfix beschreibt. Obwohl auch dieser Dienst nur lokal genutzt wird, wird er nicht als Typ *unix* definiert, sondern als *inet*. Er sorgt dafür, dass Postfix die geprüften Mails von Amavis auf Port *10025* wieder in Empfang nimmt. Diese Mails sind schon auf Viren geprüft, deshalb wird die Option *-o content_filter=* leer gesetzt. Und bevor Postfix die Mails an Amavis übergibt, hat das Tool schon die Standard-Überprüfungen durchgeführt. Diese Funktionen werden deshalb an dieser Stelle abgeschaltet. Dazu dienen die dritte bis letzte Zeile dieses Konfigurations-Blocks.

Achtung: Gleichheitszeichen und Kommas dürfen keinesfall von Leerzeichen eingeschlossen sein. Denn Leerzeichen dienen in der Postfix-Konfiguration als Trennzeichen.

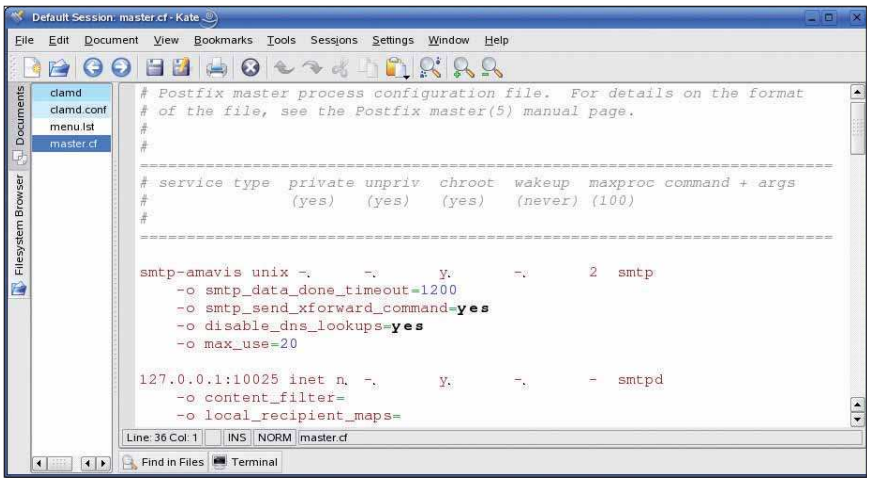
```
127.0.0.1:10025 inet n  -  y  -
-  smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o relay_recipient_maps=
     -o smtpd_restriction_clas-
ses=
     -o smtpd_delay_reject=no
     -o smtpd_client_restric-
tions=permit_mynetworks,reject
     -o smtpd_helo_restrictions=
     -o smtpd_sender_restric-
tions=
     -o smtpd_recipient_restric-
tions=permit_mynetworks,reject
     -o mynetworks_style=host
     -o mynetworks=127.0.0.0/8
     -o strict_rfc821_envelo-
pes=yes
     -o smtpd_error_sleep_time=0
     -o
smtpd_soft_error_limit=1001
     -o
smtpd_hard_error_limit=1000
     -o smtpd_client_connec-
tion_count_limit=0
     -o smtpd_client_connec-
tion_rate_limit=0
     -o receive_override_opti-
ons=no_header_body_checks,no_unk
nown_recipient_checks
```

Amavis konfigurieren

Postfix ist damit eingerichtet, nun geht es um Amavis. Das größte Problem bei der Konfiguration liegt darin, dass es verschiedene Programmversionen gibt. Die Anwendung *amavisd-new* ist kein Modul des Ama-



Wachsam: Der Antivirus-Daemon »clamd« überwacht sowohl Mails als auch Dateizugriffe



Tückisch: Bereits ein falsches Zeichen in den Postfix-Konfigurationsdateien kann genügen, um den Postversand scheitern zu lassen

vis-Pakets. Vielmehr handelt es sich dabei um eine Fork aus der Entwicklungslinie, die sich unter *www.ijs.si/software/amavisd/* als ganz neues Produkt präsentiert. Es ist die aktuellste Version und wird daher in diesem Workshop verwendet. Diese Info sollten Sie im Hinterkopf behalten, wenn Sie im Internet nach weiterführenden Informationen und Workarounds zu Amavis suchen.

Die Einstellungen zu Amavis finden Sie in */etc/amavisd.conf*. Stellen Sie dort die Variable *$myhostname* auf Ihre Domain ein. Bei Problemen gibt sich Amavis zunächst recht einsilbig. Sie können dem Programm aber mehr Informationen entlocken, indem Sie die Variable *$log_level* auf einen höheren Wert setzen. Bei der höchsten Einstellung – fünf – geizt Amavis nicht mehr mit Infos. Die komplette Spanne der Hinweise finden Sie in der Datei */var/log/amavisd.log*.

Voreinstellungen testen

Die Konfigurationsdatei von Amavis enthält bereits Voreinstellungen für ein gutes Dutzend gängiger Virenscanner. Diese Programme versucht die Anwendung beim Start automatisch einzubinden. Ob das im Einzelfall auch wirklich gelungen ist, können Sie mit *grep* herausfinden:

```
grep Found.*"av scanner"
  /var/log/amavisd.log
Aug  4 01:05:43 links.it-
  journalist.de /usr/sbin/
  amavisd[4830]: Found secondary
  av scanner ClamAV-clamscan
  at /usr/bin/clamscan
```

Troubleshooting

Um festzustellen, ob ClamAV, Amavis und Postfix reibungslos laufen, verwenden Sie nacheinander die folgenden Befehle:

```
rcclamd status
rcpostfix status
rcamavis status
```

Die Antwort *running* signalisiert, dass die Dienste funktionieren. Ob Amavis und Postfix auf den richtigen Ports erreichbar sind, finden Sie mit diesem Telnet-Befehl heraus:

```
telnet localhost 10024 -
  Connected to amavisd-new
  service ready
  telnet localhost 10025 -
  Connected to ESMTP Postfix
```

Über beide Dienste sollten Sie E-Mails per Telnet-Übertragung senden können:

```
telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-
  new service ready
MAIL FROM:root
250 2.1.0 Sender root OK
RCPT TO:achim@rechts.home
250 2.1.5 Recipient
achim@rechts.home OK
DATA
354 End data with
  <CR><LF>.<CR><LF>
Test
.
250 2.6.0 Ok, id=08114-01, from
  MTA([127.0.0.1]:10025): 250
  Ok: queued as BB6DE3C857
quit
221 2.0.0 [127.0.0.1] amavisd-
  new closing transmission
  channel
Connection closed by foreign
  host.
```

Kontrolle der Warteschlange

Versenden Sie per Script mehrere Testmails auf einen Schlag, ist es sinnvoll, die Mail-Warteschlange immer wieder mit *mailq* zu kontrollieren. Sammeln sich dort zu viele verzögerte Mails an, leeren Sie die Warteschlange mit *postsuper -d ALL*. Weitere Details zur Verbindung zwischen Postfix und

Übersicht: Antivirenprogramme für Amavis

Neben ClamAV kann Amavis auch eine ganze Reihe kommerzieller Antivirenprodukte einbinden. In dieser Übersicht stellen wir Ihnen eine Auswahl von Produkten vor, für die deutschsprachiger Support verfügbar ist.

Produkt	ClamAV	AVG	Avira Antivir UNIX	F-Prot	Dr. Web	AVP	eTrust Antivirus
Hersteller	ClamAV Team	Grisoft	Avira	Frisk	Doctor Web	Kaspersky	CA
Deutscher Support	u. a. Blasberg Computer Systeme	Jakob Software	Avira	Percomp Verlag	InSoft EDV-Systeme	Kaspersky GmbH	CA Deutschland
Preis	kostenlos	ab 195 Euro	ab 310 Euro	ab 130 Dollar	ab 150 Euro	ab 280 Euro	ab 400 Dollar
Laufzeit	unendlich	2 Jahre	1 Jahr	1 Jahr	1 Jahr	1 Jahr	1 Jahr
Homepage www.	clamav.net	grisoft.de	avira.de	f-prot.com	sald.com	kaspersky.com	www3.ca.com/Solutions/Product.asp?ID=156

Amavis finden Sie im Amavis-Paket in der Datei *README.postfix*. Sie ist bei Suse unter */usr/share/doc/packages/amavisd-new/README_FILES/* zu finden. Im Web steht ebenfalls eine Kopie bereit: *www.ijs.si/software/amavisd/README.postfix.txt*.

Wenn der Mail-Server mit Virenschutz rund läuft, sollten Sie noch die Dämonen *amavisd* und *clamd* in den Systemstart einbinden. Unter Suse ist das mit dem Runlevel-Editor von Yast schnell erledigt.

Im letzten Schritt richten Sie den cronjob ein, der die Virensignaturen im Stundenrhythmus auf den neusten Stand bringt.

Dateiserver härten

Um einen Dateiserver vor Virenbefall schützen zu können, muss sich das Antivirenprogramm direkt in die Dateizugriffe einklinken. Für Server vom Typ Samba und Netatalk hat sich das Kernel-Modul Dazuko bewährt, das ursprünglich von Avira stammt (früher H+B EDV) und unter *dazuko.org* heruntergeladen werden kann. Kleines Manko des kostenlosen Tools: NFS-Dateien kann es derzeit noch nicht schützen.

Hilfreich: Mit Suse Linux 10.1 werden mehrere vorkompilierte Dazuko-Module geliefert, die mit den jeweiligen Kernel-Varianten funktionieren. Unter anderen Distributionen muss das Modul mit den aktuellen Kernel-Quellen kompiliert werden.

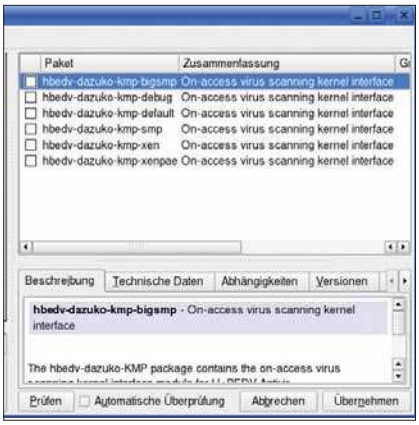
Virtuelles Device

Zunächst wird mit *mknod -m 600 /dev/dazuko c 254 0* ein Device für Dazuko erzeugt. Benutzer und Gruppe für das Gerät werden auf *root* gesetzt. Dann kopieren Sie das Modul *dazuko.ko* in den Ordner, der auch die anderen Kernel-Module enthält. In die Konfigurationsdatei für die Module fügen Sie die Zeile *alias char-major-254 dazuko ein*. Die Konfiguration finden Sie je nach Distribution beispielsweise unter */etc/modules.conf* oder */etc/modprobe.conf.local*. Schließlich können Sie das Modul mit dem Befehl *modprobe dazuko* in den Kernel laden und den Ladevorgang mit *lsmod|grep dazuko* überprüfen.

Suse Linux macht Probleme

Unter Suse klappt die Einbindung nicht immer reibungslos. Je nach Suse-Version weigert sich *modprobe*, das Modul zu laden. Auf diese Weise geht es trotzdem:

Befindet sich das Kernel-Modul *dazuko.ko* im Ordner für die Kernel-Module, erneuern Sie die Modulabhängigkeiten mit *depmod -a*. Deaktivieren Sie dann SELinux, indem Sie die Grub-Startoptionen unter



Sicherheit an Bord: Das Kernel-Modul Dazuko gehört zum Lieferumfang von Suse Linux 10.1

/boot/grub/menu.1st ändern. Suchen Sie den Eintrag für die aktuelle Kernel-Version und fügen Sie am Ende der Zeile den Befehl *selinux=0* hinzu. Das sieht zum Beispiel so aus:

```
title SUSE Linux 10.1
root (hd1,8)
kernel (...Auslassungen...)
  showopts selinux=0
```

Startoptionen definieren

Dann ändern Sie die Startoptionen des Kernels so, dass Dazuko geladen wird. In der Datei */etc/sysconfig/kernel* finden Sie einen Eintrag *MODULES_LOADED_ON_BOOT=""*. An diese Stelle fügen Sie mit diesem Befehl die Dazuko-Option ein:

```
MODULES_LOADED_ON_BOOT=
  "dazuko capability"
```

Beim nächsten Neustart wird Dazuko dann automatisch geladen. Nicht vergessen: ClamAV kann nur auf Dazuko zugreifen, wenn es als *root* gestartet wird. Dazu deaktivieren Sie in der Datei */etc/clamd.conf* die Option *User vscan*.

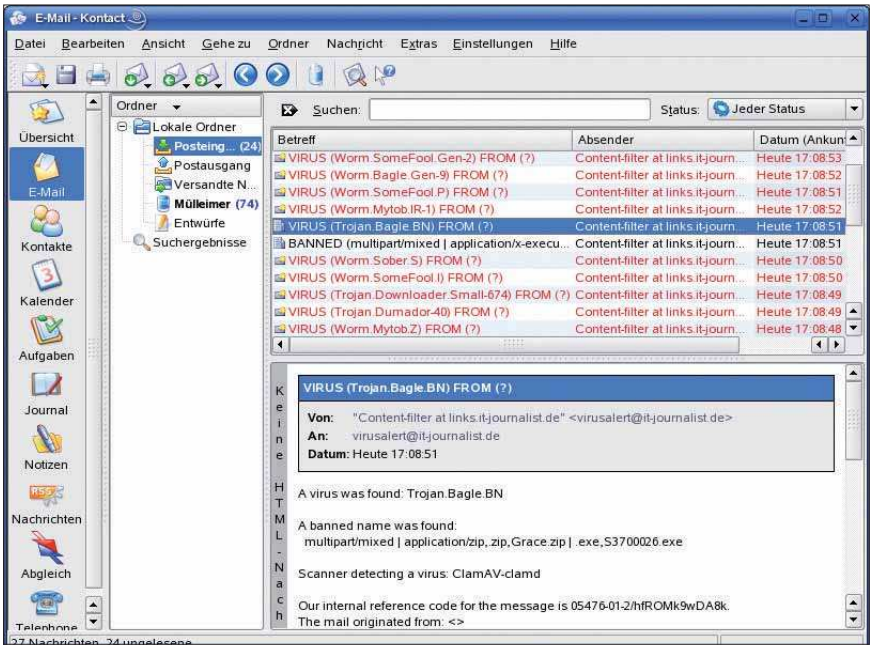
Am Ende der Konfigurations-Datei teilen Sie *clamd* mit folgendem Block mit, welche Ordner es schützen und wie das Programm dabei vorgehen soll:

```
ClamukoScanOnAccess
ClamukoScanOnOpen
ClamukoScanOnClose
ClamukoScanOnExec
ClamukoIncludePath /
ClamukoExcludePath /proc
ClamukoExcludePath
/var/spool/amavis
```

In diesem Beispiel wird der komplette Server überwacht – mit zwei Ausnahmen. Wichtig ist vor allem die letzte Zeile. Hier wird die Mail-Warteschlange von Amavis von der Prüfung ausgenommen. Würde Dazuko diese Dateien blockieren, könnte Amavis keine Mails mehr prüfen. Der Test zeigt, dass neben ClamAV auch Grisofts AVG gut mit Dazuko zusammenarbeitet.

Der Aufwand lohnt sich

Es ist nicht einfach, mit Postfix, Amavis, Dazuko und ClamAV die Server-Sicherheit zu erhöhen. Als Problem erweist sich die Verbindung zwischen Postfix und Amavis. Sind die Komponenten aber installiert und konfiguriert, sind Mail- und Dateiserver zuverlässig gegen Viren geschützt. ■



Alarm: Der Versender von Virenmails wird automatisch benachrichtigt, sofern der Virus nicht seine Absenderadresse gefälscht hat