

Virenschutz in der Linux Musterlösung (ML)

Die Bedeutung des Wortes (Computer-)Virus wird unter <http://www.net-lexikon.de/Virus.html> definiert als „in böswilliger Absicht geschriebener Programm-Code ...“. Leider geht der Virenbefall eines Computers meistens nicht so glimpflich aus wie beim „Amish Virus“ (siehe Kasten rechts). Auf Virenschutz sollte deshalb besser nicht verzichtet werden.

In der Linux ML stehen grundsätzlich drei Möglichkeiten zum Schutz gegen Viren zur Verfügung:

1. **Virens Scanner auf den Client-Rechnern installieren**
2. **Virens Scanner auf dem Server installieren**
3. **E-Mail Virens Scanner auf dem Server installieren**



Dass auf Virenschutz besonders auch im schulischen Umfeld nicht verzichtet werden kann ist wohl unbestritten. Frage ist nur welche Alternative ist am kostengünstigsten, sichersten und gleichzeitig nicht so wartungsaufwendig. Im Folgenden werden die genannten Alternativen erläutert. Gleichzeitig erfolgt eine grobe Beschreibung der notwendigen Installationsschritte zur Integration in die Linux ML (ab Version 2.0). Die Beschreibung bezieht sich hier auf die nicht kommerziellen Versionen der Virens Scanner, die jedoch nur im privaten Umfeld kostenlos verwendet werden dürfen. Die Übertragung auf die kommerziellen Versionen, die teilweise mehr Funktionen bieten, sollte aber nicht schwer fallen.

1. **Virens Scanner auf den Client-Rechnern installieren:**

Die einfachste Lösung ist zunächst, wie zu Hause einfach einen Virens Scanner auf dem Windows-Client zu installieren. Bei AntiVir Guard für Windows erfolgt der Download des Virens Scanners nach erfolgter Anmeldung unter <http://www.free-av.de/>.

Lediglich im privaten Bereich ist dieser Virens Scanner kostenlos. Für den schulischen Einsatz sind Lizenzgebühren zu entrichten und die kommerzielle Version des Virens Scanners sollte unter <http://www.antivir.de/> verwendet werden. Aktuelle Angaben findet man unter den genannten Internetadressen.

Besondere Stärke des Virens Scanners ist u.a. das automatische Internetupdate der Signaturdatei. Alle 14 Tage fordert der Virens Scanner zum Update auf und holt sich aus dem Internet aktuelle Programmversionen und Signaturdateien zum Schutz gegen die neuesten Viren.

In Verbindung mit der Linux ML muss dieses Update aber nicht an jedem einzelnen Client durchgeführt werden: Es genügt alle 14 Tage an einem Musterclient das Signaturupdate durchzuführen und danach ein inkrementelles Image der Installation zu erzeugen. Die anderen Clientrechner erhalten dann bei der nächsten Restauration alle geänderten Dateien (Siehe Kasten Restauraionskonzept bei der Linux ML).

Die beschriebene Vorgehensweise kann natürlich mit jedem anderen Virens Scanner für Windows durchgeführt werden.

2. **Virens Scanner auf dem Server installieren:**

Virenschutz auf dem Client alleine genügt nicht. Zwar kann dadurch weitgehend ausgeschlossen werden, dass durch die Benutzer Viren vom Client auf den Server kommen. Die Gefahr des Virenbefalls des Servers entweder bei Aktivitäten des Administrators oder direkt aus dem Internet ist dadurch aber noch nicht beseitigt.

Deshalb ist es sinnvoll einen Virens Scanner auf dem Server zu installieren. Die Vorgehensweise bei der Linux ML (ab Version 2.0) wird hier für F-Prot Antivirus für Linux beschrieben. Prinzipiell kann aber jeder andere Virens Scanner für Linux eingesetzt werden.

Lediglich im privaten Bereich ist dieser Virens Scanner kostenlos. Für den schulischen Einsatz sind Lizenzgebühren zu entrichten. Aktuelle Angaben findet man unter der Internetseite

<http://www.f-prot.com>.

Nach erfolgter Benutzerregistrierung auf dieser Internetseite kann das Programmpaket fp-linux-ws-VERSION.rpm (hier: Workstationversion, für den kommerziellen Einsatz existiert auch eine File Server und eine E-Mail Server Version) herunter geladen und auf dem Server (als root) mit

dem Befehl `rpm -Uhv fp-linux-ws-VERSION.rpm` installiert werden. Diese beiden Schritte entfallen, wenn bei der Installation der Linux Musterlösung (ab Version 2.2) bereits die Installation von F-Prot ausgewählt wird.

Der Virenschanner ist nun einsatzbereit und kann aufgerufen werden:

- Versionsinformationen anzeigen: `/usr/local/f-prot/f-prot -verno`
- Password-File nach Viren scannen: `/usr/local/f-prot/f-prot /etc/passwd`
- Test des Virenschanners: EICAR_TEST_FILE erzeugen und scannen.
Die Erzeugung der Testdatei wird unter http://www.f-prot.com/support/helpfiles/unix/linux_ws/test_eicar.html beschrieben.

Damit der Virenschanner in regelmäßigen Zeitabständen nach Viren auf dem Server sucht, muss lediglich in der Datei `/etc/crontab` der Eintrag

```
1 6 * * * root /usr/local/f-prot/f-prot -silent -report=/var/log/f-prot.log -append -auto -disinf /
```

hinzugefügt werden. Dann wird jeden Morgen um 6:01 Uhr nach Viren gescannt und bei infizierten Dateien wird versucht den Virus zu entfernen. Das Logfile wird in der Datei `/var/log/f-prot.log` abgespeichert. Die Bedeutung der angegebenen und noch weiterer Befehlsparameter von F-Prot findet man im Internet unter

http://www.f-prot.com/support/helpfiles/unix/linux_ws/scanning_options.html und

http://www.f-prot.com/support/helpfiles/unix/linux_ws/reporting_options.html.

Bei der Angabe des Pfades `/` wird der gesamte Server inklusive aller Netzlaufwerke der Benutzer durchsucht. Von den Clients auf dem Server abgespeicherte Viren werden also ebenfalls erkannt. Lediglich die lokalen Laufwerke der Clients können so nicht erfasst werden. Bei aktivierter automatischer Restauration der Clients in der Linux ML (ab Version 2.0) werden eventuell vorhandene Virendateien beim Booten des Rechners aber sowieso entfernt, so dass ein Virenschanner auf dem Clientrechner nicht unbedingt benötigt wird.

Möchte der Administrator eine bestimmte Datei nach Viren scannen, so kann dies von jedem beliebigen Rechner im Schulnetz aus erfolgen. Dazu muss lediglich einmal ein entsprechender Webmin Eintrag definiert werden. Mit einem Internetbrowser ist es dann möglich auf diesen Eintrag zuzugreifen und die Virensuche zu starten (siehe Kasten Serververwaltung mit Webmin).

Soll nach dem täglichen Virenschannen der Administrator informiert werden, kann beispielsweise mit folgendem crontab Eintrag um 6:30 Uhr eine E-Mail an admin verschickt werden:

```
30 6 * * * root /usr/bin/grep "Infection" /var/log/f-prot.log > /usr/bin/mail -s VIRUS admin; mv /var/log/f-prot.log /var/log/f-prot.log.sav
```

Wie bei der Clientinstallation ist ein regelmäßiges Update der Signaturdatei erforderlich. Bei bestehender Internetverbindung erfolgt dies durch Eingabe des Befehls:

```
/usr/local/f-prot/tools/check-updates.pl
```

Auch hier kann durch einen entsprechenden Eintrag in der Datei `/etc/crontab` das Signaturupdate in regelmäßigen Zeitabständen vom System automatisch ausgeführt werden.

Beispielintrag: An jedem Monatsersten wird um 6:01 Uhr das Signaturupdate durchgeführt:

```
1 6 1 * * root /usr/local/f-prot/tools/check-updates.pl -cron
```

Genauso kann auch ein Webmin Eintrag zum manuellen Starten des Updates vorgenommen werden.

Auch das Erstellen von crontab Einträgen kann mit Hilfe von Webmin durchgeführt werden:

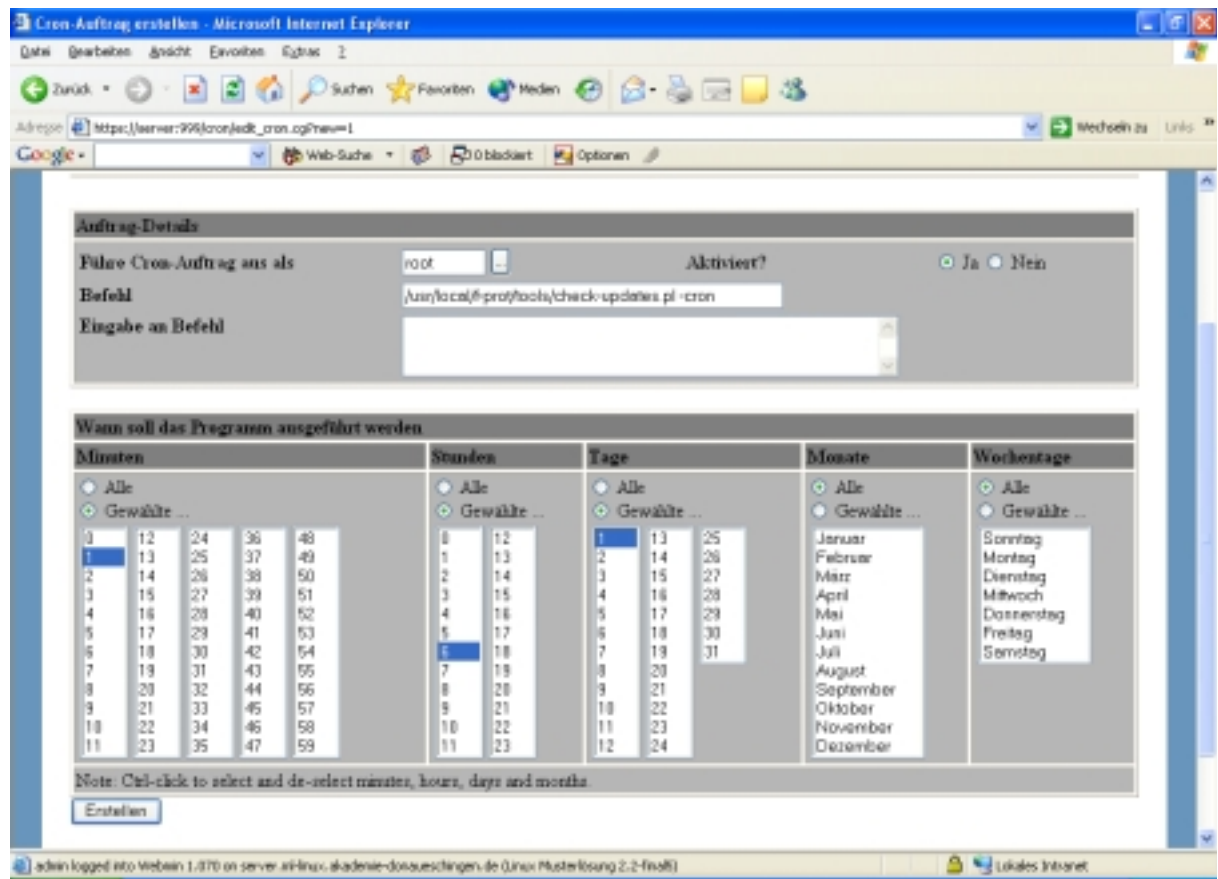
Im Menü

System → Geplante Cron-Aufträge → Neuer geplanter Cron-Auftrag erstellen

können der auszuführende Befehl, der Benutzer und der Ausführungszeitpunkt weitgehend menübasiert festgelegt werden.

Webmin speichert den cronjob aber nicht in `/etc/crontab` sondern in den benutzerspezifischen crontabs ab. Beispielsweise für den Benutzer root in `/var/spool/cron/tabs/root`.

In der folgenden Abbildung ist der entsprechende Webmin-Dialog für den crontab Eintrag des Signaturupdates dargestellt:



3. E-Mail Virenschanner auf dem Server installieren:

Um eingehende oder versendete E-Mails auf dem Server nach Viren zu scannen kann mit Hilfe des in der Linux ML vorhandenen AMaViS Programms („A Mail Virus Scanner“) der in 2. installierte Virenschanner verwendet werden. AMaViS schaltet sich dazu in das E-Mail-System ein und überprüft mit Hilfe vorhandener Virenschanner die vom sendmail-Dienst auszuliefernden Nachrichten und Dateien auf Viren.

Wird bereits bei der Installation der Linux Musterlösung (ab Version 2.2) die Aktivierung von AMaViS ausgewählt, müssen die folgenden Schritt nicht mehr durchgeführt werden.

Ob AMaViS auf dem System bereits aktiviert ist, kann man in der Datei

/etc/rc.config

überprüfen. Dort sollte der Eintrag

START_AMAVIS="yes"

vorhanden sein. Falls das nicht der Fall ist muss der Eintrag geändert werden und danach AMaViS mit dem Befehl

rcamavis start

gestartet werden.

Danach ist in der Datei

/etc/sendmail.cf

noch ein zusätzlicher Eintrag notwendig: (Bevor dieser Eintrag hinzugefügt werden kann, sollte das E-Mail-System durch rsendmail stop angehalten werden.)

sendmail.cf, Zeile 530

O InputMailFilters=milter-amavis

Xmilter-amavis, S=local:/var/amavis/amavis-milter.sock, F=T, T=S:10m;R:10m;E:10m

Mit

rsendmail start

wird das E-Mail System wieder gestartet. Erscheinen hier Fehlermeldungen, sollte man die in sendmail.cf vorgenommenen Änderungen nochmals genau überprüfen!

Bei Versenden einer infizierten E-Mail oder eines infizierten E-Mail-Attachments erhält nun der Versender und der Administrator (admin) einen entsprechenden Hinweis per E-Mail. Die infizierte E-Mail wird in das Verzeichnis

/var/spool/vscan/virusmails

verschoben und nicht versendet.

Entsprechende Tests können wieder mit dem EICAR-Testfile (s.o.) durchgeführt werden.

Selbstverständlich können hier nur die E-Mails nach Viren gescannt werden, die von auf dem Server vorhandenen E-Mail Accounts ausgehen bzw. an diese geschickt werden. Der komplette schulische E-Mail Verkehr muss dann also über diesen Server abgewickelt werden. Durch Bereitstellung der pop3 und smtp-Dienste durch den Server können die Clients aber weiterhin ihre E-Mails auch lokal unter Windows bearbeiten.

Für welche Alternative man sich nun entscheidet hängt sicherlich auch noch von individuellen schulischen Bedürfnissen ab. Verwendet man die in der Linux ML (ab Version 2.0) mögliche automatische Restauration der Clients beim Booten, kann man auf Virens Scanner bei den Clientrechnern eventuell verzichten. Gleichzeitig entfällt dadurch der Aufwand für regelmäßige Signaturupdates und die Lizenzgebühren für die Client-Virens Scanner. Auftauchende Viren, beispielsweise von Benutzern auf Diskette mitgebrachte, werden diesen selbst zwar nicht sofort angezeigt. Der Administrator erhält aber für die Netzlaufwerke eine entsprechende Nachricht durch den Virens Scanner am Server, die er bei Bedarf weiterleiten kann. Lokal auf der Festplatte des Clients abgelegte Viren werden durch die automatische Restauration beim nächsten Booten gelöscht. Eine Rückmeldung zum Benutzer erfolgt hier aber nicht.

Wer auf eine solche Rückmeldung nicht verzichten möchte, kommt um einen Virens Scanner am Client nicht herum. Einige kommerzielle Virens Scanner sind sogar in der Lage die Signaturdatei des Clients automatisch vom Server zu beziehen, so dass diese nur einmal aus dem Internet herunter geladen werden muss.

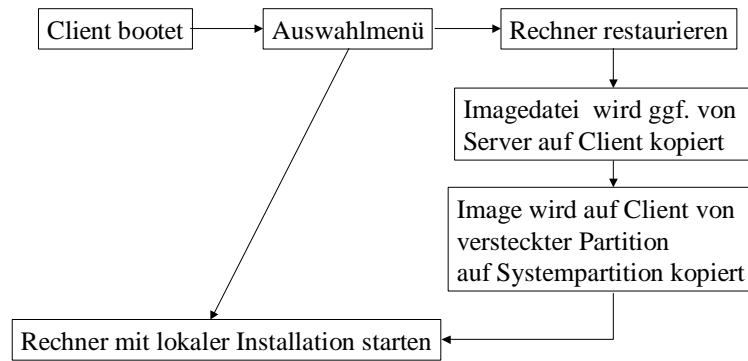
Auf einen Virens Scanner am Server sollte man aber keinesfalls verzichten. In Kombination mit AMaViS kann dadurch gleichzeitig kostenlos der schulische E-Mail-Verkehr nach Viren durchsucht werden. Die kommerziellen Virens Scanner werden in unterschiedlichen Versionen angeboten: Neben der Workstation- und File Server-Version kann man (gegen Aufpreis) ebenfalls direkt einen E-Mail Virens Scanner bestellen. Aktuelle Informationen zu den Lizenzgebühren sind über die angegebenen Internetseiten verfügbar.

Andrea und Marco Neumann

Nützliche Quellenangaben zur Linux Musterlösung:

- Dokumentation zur Linux ML:
<http://www.support-netz.de/dt/lml-dokumentation.html#Installation>
- Archiv der LinuxMailingliste:
<http://mailman.schule-bw.de/pipermail/linuxmuster>
- AMaViS Homepage:
<http://www.amavis.org/>
- AntiVir Homepage:
privat: <http://www.free-av.de/> kommerziell: <http://www.antivir.de/>
- F-Prot Homepage: <http://www.f-prot.com>

Restaurationskonzept bei der Linux ML:



Neuerungen ab Version 2.0:

- Restauration bei jedem Booten auch automatisch ohne Auswahlmenü möglich
- Dabei wird nicht die komplette Imagedatei sondern es werden jeweils nur einzelne veränderte Dateien kopiert
- Bei der Erzeugung eines neuen Images können neben kompletten auch inkrementelle Images erzeugt werden
- Diese enthalten dann nur die gegenüber dem ursprünglichen Image neu installierte Dateien und Programme

Serververwaltung mit Webmin:

Webmin ist ein web basiertes grafisches Tool zur Administration eines Linux Servers das in der ML bereits enthalten ist. Durch Eingabe der Adresse <https://servername:999> wird Webmin gestartet.

Nach Anmeldung mit Benutzername und Kennwort kann auf beliebige Systemkommandos menü basiert zugegriffen werden.

Eigene Kommandos können als Administrator unter „Eigene Befehle“ über den Menüpunkt „Einen neuen eigenen Befehl erstellen“

definiert werden.

Beispielsweise der Aufruf des Virenschanners und der Aufruf des Signaturupdates.

