Schwerpunkt: KlamAV 0.30.3

eine Vorstellung von Dieter Schütze, 17.09.2005

Vorwort

Da immer wieder Nachfragen zu einem Virenschutz auf Linux gestellt werden, möchte ich hier mal ein unter GPL stehendes, grafisches Benutzerfrontend für KDE vorstellen.

Installation: es kommt auf die Quelle an.

Da die Pakete ClamAV und KlamAV bei Mandriva nicht aktuell sind, sollten wir nach einer anderen Quelle Ausschau halten. Sehr aktuell sind beispielsweise die Quellen von MandrivaUser.de, so möchte ich nachfolgend noch zeigen, wie diese eingebunden werden. Das verwendete System ist in diesem Fall die Mandriva LE2005, auch als 10.2 bekannt.

Quellen einbinden

Im Menü unter System, Einstellungen, Paketverwaltung wird der Paketquellen-Manager aufgerufen. Um diesen zu starten, wird das root Kennwort benötigt. Wir bekommen dann den Medien konfigurieren Dialog angezeigt.

Abbildung 1: Medien konfigurieren

In diesem ist ersichtlich, welche Quellen schon eingebunden sind. Um eine neue Quelle einzubinden, müssen wir in unserem Fall die Schaltfläche Füge angepaßte hinzu... auswählen. Im nächsten Dialog mit dem Namen Medium hinzufügen geben wir die notwendigen Daten für die Quelle ein.

Abbildung 2: Medium hinzufügen

Beim Mediumstyp aktivieren wir die Option FTP-Server, und unter Name vergeben wir einen Namen für die Quelle. Da ich die freien Quellen von MandrivaUser.de benutze, nenne ich diese *mud-free*.

Unter URL wird die Adresse der Quelle angegeben, die in diesem Beispiel ftp://mandrivauser.de/rpm/GPL/2005/RPMS/ lautet. Diese Adresse zeigt einfach auf die ganzen rpm-Pakete. Ein relativer Pfad zu der Synthesis oder hdlist ist in diesem Fall nicht notwendig, da sich diese im gleichen Pfad wie die Pakete befinden. Nach Ok wird sogleich die Medienquelle hinzugefügt. Diese sollte dann im Dialog „Medien konfigurieren“ mit dem vorgegebenen Namen angezeigt werden.

KlamAV installieren

Zum Installieren von KlamAV wählen wir im Startmenü unter System, Einstellungen, Paketverwaltung den Eintrag Software installieren. Auch hier muß das root-Kennwort eingegeben werden, worauf sich der Dialog RpmDrake öffnet.

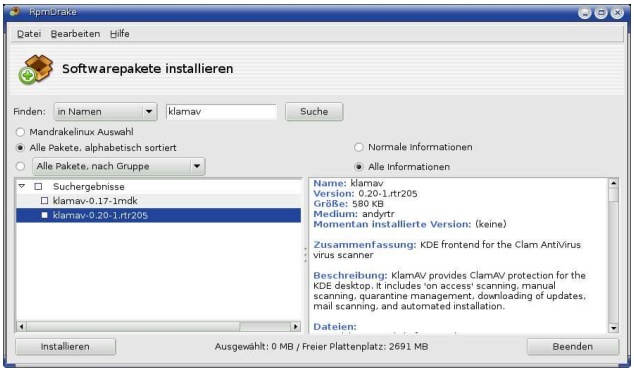


Abbildung 3: RpmDrake

Jetzt lassen wir das gewünschte Paket suchen und geben im Finden Feld einfach klamav ein und betätigen die Suche Schaltfläche. Als Ergebnis sollten nun alle verfügbaren KlamAV Pakete angezeigt werden. Hier sehen wir auch gleich, dass die Version von Mandriva veraltet ist und setzen ein Häckchen bei der aktuellen Version. Es erscheint ein zusätzlicher Dialog, der uns die zusätzlich notwendigen Pakete anzeigt und den wir mit Ok bestätigen.

Abbildung 4: zusätzliche Pakete

Danach im RpmDrake Dialog die Schaltfläche installieren auswählen. Hierauf werden sogleich die Pakete heruntergeladen und installiert

Abbildung 5: Installation

KlamAV verwenden

Im Startmenü unter System Dateiwerkzeuge befindet sich jetzt ein Eintrag „KlamAV“, den wir nun auswählen.

Erster Start und notwendige Schritte

Es ist soweit, wir bekommen zum ersten Mal das grafische Frontend für KDE, KlamAV, zu sehen.

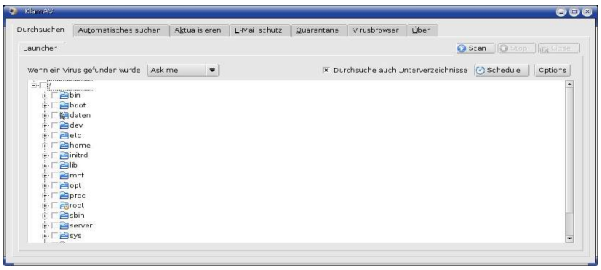


Abbildung 6: Durchsuchen

Bevor wir nun richtig loslegen, sollten wir zuerst die aktuellen Virensignaturen herunterladen und wähen hierfür die Registerkarte Aktualisieren aus.

Abbildung 7: Aktualisieren

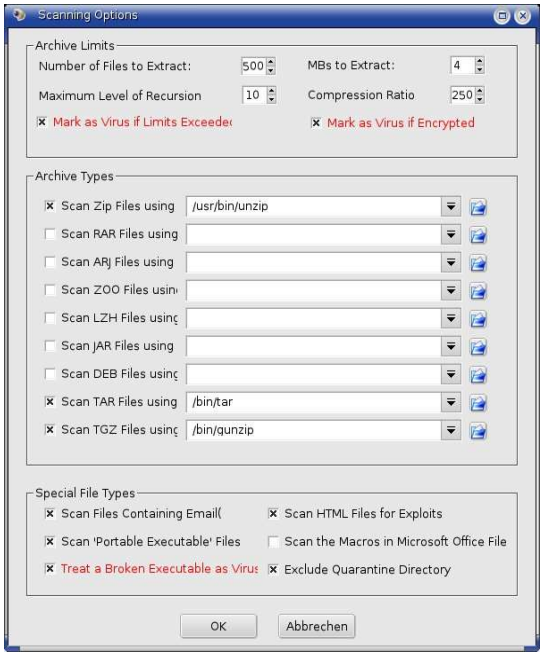
Da das Ganze unter dem Benutzerzugang läuft, befindet sich die Virensignaturdatenbank im eigenen Home Verzeichnis. Wer einen systemweiten, übergreifenden Virenschutz benötigt, sollte sich den ClamAV-Artikel auf www.mandrivauser.de anschauen.

Unter Software Updates lassen sich ClamAV und KlamAV aktualisieren. Hierzu kann ausgewählt werden, dieses automatisch über KlamAV zu erledigen. Mit den Knöpfen Upgrade ClamAV oder Upgrade KlamAV kann die Software direkt aktualisiert werden. Wer einen vorgeschalteten Proxy hat (wird bei den wenigsten der Fall sein), sollte im Abschnitt Proxy die notwendigen Daten eingeben. Unter AutoUpdate Settings kann eingestellt werden, wie oft am Tag die Signaturen aktuallisiert werden.

Benutzer, die keine Flatrate für Ihren Internetzugang besitzen, sollten diese Option besser deaktivieren und die Signaturen manuell laden. Für alle gilt, dass beim ersten Start die Signaturen manuell geholt werden sollten. Dies wird über die Schaltfläche jetzt aktualisieren erledigt. Wenn diese nicht anwählbar ist, sind die Signaturen aktuell. Unten in der Statuszeile kann das Holen der Signaturen beobachtet werden.

KlamAV Optionen

Fangen wir nun bei der ersten Registerkarte Durchsuchen an. Dort sollten zunächst einmal die Options eingestellt werden.



Die unterschiedlichen Optionen von oben nach unten:

Number of Files to Extract
bedeutet die Anzahl der Dateien, die aus einem Archiv entpackt und untersucht werden sollen.
MBs to Extract
Wie groß dürfen die zu untersuchenden Archive maximal sein.
Maximum Level of Recursion
Wie tief soll in das Archiv maximal rekursiv gescannt werden (Verzeichnistiefe)
Compression Ratio
Die Kompressionsrate in Prozent, die ein Archiv maximal haben darf. Schützt vor sogenannten Mailbomben, also Archive die gepackt einige Kilobytes haben und nach dem Entpacken mehere Gigabytes groß sind.
Mark as Virus if Limits Exceeded
Wenn einer der gesetzten Limits überschritten wird, wird dieses Archiv als Virus markiert.
Mark as Virus if Encrypted
Ist das Archiv verschlüsselt, wird es als Virus markiert. Bei Archive Types werden die zu untersuchenden Archivarten ausgewählt. Zusätzlich ist noch das Programm anzugeben, mit dem diese Archive entpackt werden sollen.

Jetzt noch die Rubrik Special File Types :

Scan Files Containing Email
Dateien die E-Mails enthalten, sollen auch gescannt werden (mime-codiert e.t.c.)
Scan HTML Files for Exploits
Durchsuche HTML Dateien
Scan Portable Executable Files
EXE, DLL, OBJ und andere Dateitypen.
Scan the Macro in Microsoft Office File
Die beliebten Makros in Microsoft Office Dateien
Treat a Broken Executable as Virus
Behandle eine zerstörte ausführbare Datei als Virus
Exclude Quarantine Directory
Das Quarantäneverzeichnis soll vom scan ausgeschlossen werden.

Manuelles Durchsuchen

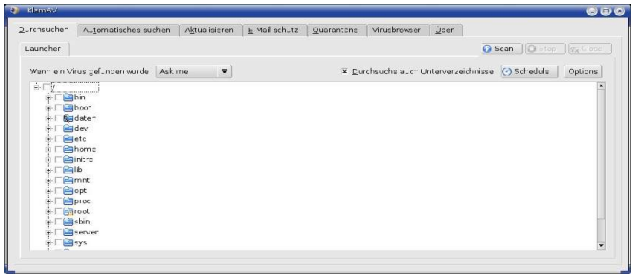


Abbildung 8: manuelles durchsuchen

Sind alle notwendigen Optionen gesetzt, kann mit dem ersten manuellen Scannen begonnen werden. Hierzu wählen wir ein oder mehrere Verzeichnisse aus und können noch die Option Wenn ein Virus gefunden wurde bestimmen. Es gibt drei Möglichkeiten der Behandlung:

1. Ask me
   KlamAV wird dann den Benutzer fragen, was er mit der gefundenen Datei machen soll.
2. Quarantine File
   KlamAV verschiebt die befallene Datei in die Quarantäne.
3. just report
   mit dieser Option bekommt man nur einen Bericht, die Datei bleibt, wo sie ist.

Auf jeden Fall sollte die Option Durchsuche auch Unterverzeichnisse gesetzt werden, da ansonsten nur im obersten ausgewähltem Verzeichnis nach Viren gesucht wird. Durch einen Klick auf die Schaltfläche „Scan“ geht die Virensuche los.

Wurde ask me ausgewählt, bekommt man bei einem Befund einen Dialog, in dem gefragt wird, ob die befallenen Dateien in die Quarantäne verschoben werden sollen. Hierbei werden auch die betroffenen Dateien mit Begründung angezeigt.

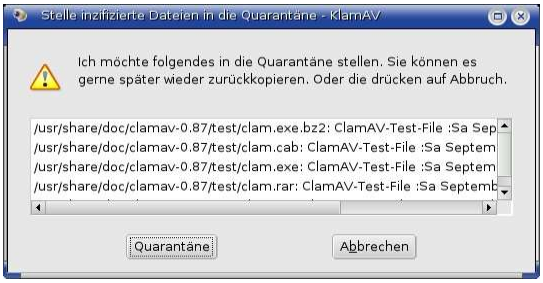


Abbildung 9: Quarantäne Meldung

Des Weiteren steht nach dem Scannen eine weitere Registerkarte mit der Bezeichnung des Durchsunungsdatums und der Uhrzeit zur Verfügung. In dieser werden alle möglicherweise befallenen Dateien nochmals aufgeführt.

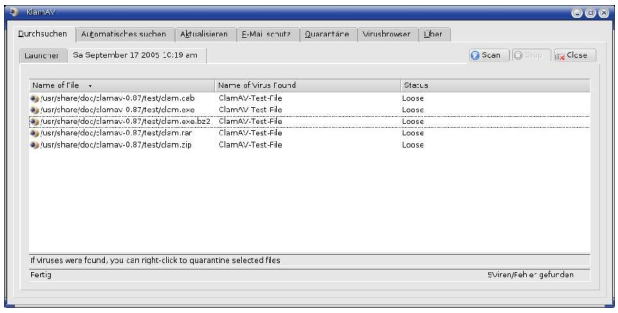


Abbildung 10: verdächtige Dateien

Durch einen Rechtsklick auf eine angegebene Datei öffnet sich eine weitere Auswahl mit den Möglichkeiten, diese Datei entweder in die Quarantäne zu verschieben oder nach dem Virus im Viruspool, bei TrendMicro oder bei Google zu suchen.

Zeitgesteuertes Durchsuchen

Unter der Registerkarte Durchsuchen gibt es noch den Schedule Knopf, womit wir beim zeitgesteuerten Scannen sind.

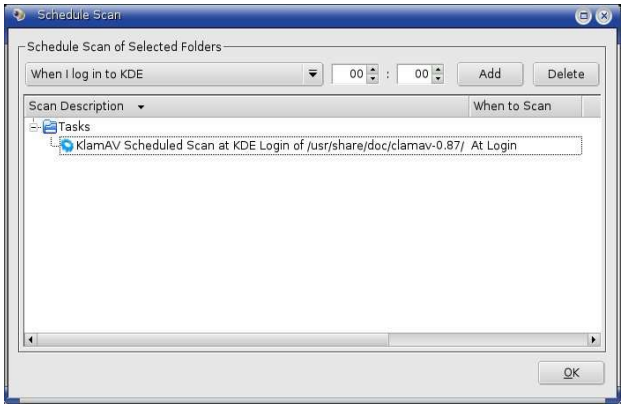


Abbildung 11: zeitgesteuertes durchsuchen

Gleich in der ersten Auswahl kann eingestellt werden, zu welcher Bedingung durchsucht werden soll:

When I log in to KDE = Beim Einloggen in einer KDE Sitzung
Every day at = Jeden Tag um (die Uhrzeit ist rechts daneben auszuwählen)
Every day at the current time = Jeden Tag zur derzeit aktuellen Uhrzeit
Every week from now on at the current time = Jede Woche von jetzt an zur derzeit aktuellen Uhrzeit
Every week from now on at = Jede Woche von jetzt an um (die Uhrzeit ist rechts daneben auszuwählen)
Every week from a specific date at = Jede Woche zu einem bestimmten Datum um (die Uhrzeit ist rechts daneben auszuwählen, zudem wird ein Kalender zur Auswahl des Datums angezeigt)
Every month from now on at the current time = Jeden Monat von jetzt an zur derzeit aktuellen Uhrzeit
Every month from now at = Jeden Monat von jetzt an um (die Uhrzeit ist rechts daneben auszuwählen)
Every month from a specific date at = Jeden Monat von einem bestimmten Datum um (die Uhrzeit ist rechts daneben auszuwählen, zudem wird ein Kalender zur Auswahl des Datums angezeigt)
Once only on a specific date at the current time = Nur einmal zu einem bestimmten Datum zur derzeit aktuellen Zeit (es wird ein Kalender zur Auswahl des Datums angezeigt)
Once only on a specific date at = Nur einmal zu einem bestimmten Datum um (die Uhrzeit ist rechts daneben auszuwählen, zudem wird ein Kalender zur Auswahl des Datums angezeigt)

Durch ein Add wird die Aufgabe hinzugefügt, und durch ein Markieren einer bestehenden Aufgabe mit nachfolgendem Delete wird eine Aufgabe gelöscht. Im Fenster unter dem Ordnersymbol „Tasks“ werden dann die eingestellten zeitgesteuerten Scans angezeigt.

Bei Zugriff durchsuchen

Die Registerkarte Automatisches suchen (on access oder bei Zugriff) funktioniert auf Mandriva Systemen leider nicht ohne weiteres. Hierzu muss ein Schalter im Kernel aktiviert und dieser neu compiliert werden. Zudem wird auch noch das Dazuko Kernelmodul benötigt, welches, wenn es im System vorhanden ist, von KlamAV durch Anwählen des Knopfes Aktivieren automatisches Suchen geladen wird.

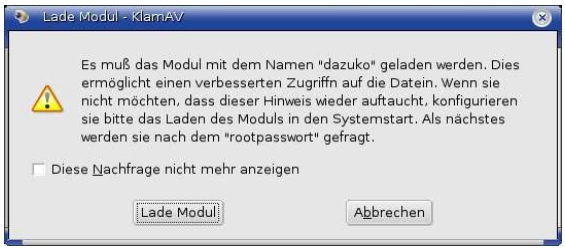


Abbildung 12: Modul laden

Da bei Mandriva Linux das Dazuko Modul nicht dabei ist und die Implementation selber durchgeführt werden muß, gibt KlamAV eine Meldung über das erfolglose Laden des Moduls aus.

Abbildung 13: nicht geladenes Modul

Dazuko und der Kernel

Dazuko ist immer noch experimentell, wer es dennoch in sein System integrieren möchte: hier eine Kurzanleitung (anzuwenden auf eigene Gefahr):

- installieren der Kernel Sourcen (urpmi kernel-source)
- wechseln in das Sourcen-Verzeichnis (cd /usr/src/linux)
- das Konfigurationsmenü für den Kernel aufrufen (make menuconfig)
- unter Security options, Enable different security modules aktivieren
- ebenfalls in den Security options die Default Linux Capabilities als Modul auswählen.
- verlassen des Dialogs und speichern nicht vergessen
- make && make modules_install && make install ausführen
- kernel in Bootmanager aufnehmen (lilo oder grub)
- editieren der /etc/modprobe.preload und folgendes einfügen:
  commoncap
  dazuko
  capability
- Neustarten mit dem neuen Kernelmodul
- Dazuko Sourcen herunterladen (http://www.dazuko.org/downloads.shtml)
- ins Verzeichnis der Dazuko Sourcen wechseln
- compilieren
  ./configure
  make
- installieren des Dazuko Moduls
  cp dazuko.ko /lib/modules/`uname -r`/kernel/security
  depmod -a
- Dazuko Modul laden
  modprobe dazuko
- erstellen eines Dazuko Devices
  mknod -m 600 /dev/dazuko c `grep dazuko /proc/devices | sed “s/ .*//“` 0
- Achtung capability und commoncap müssen geladen sein.

Sollte alles erfolgreich verlaufen sein, hier die Erläuterungen der Funktionen in KlamAV.

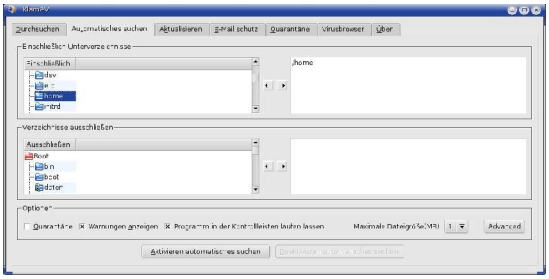


Abbildung 14: automatisches durchsuchen

In der oberen Hälfte können auf der linken Seite die Verzeichnisse ausgewählt werden die durchsucht werden sollen. In der unteren Hälfte können Verzeichnisse die aus bestimmten Gründen nicht durchsucht werden sollen ausgewählt werden. In beiden Fällen geschieht das Hinzufügen oder Entfernen durch die beiden Pfeilen in der Mitte.
Als Optionen stehen zur Verfügung:
Quarantäne = bei Befall in die Quarantäne verschieben.
Warnungen anzeigen = bei Befall eine Warnung anzeigen.
Programm in der Kontrolleiste laufen lassen = KlamAV wird an die Kontrolleiste angedockt.
Maximale Dateigröße = die maximale Dateiegröße in MB.
Advanced = erweiterte Optionen.

Bei den erweiterten Optionen stehen zur Verfügung:

Abbildung 15: erweiterte Optionen

Durchsuche Dateien wenn diese:
Created/Modified = erstellt oder verändert wurden.
Opened = geöffnet werden
Executed = ausgeführt werden
Closed = geschlossen werden
Als Archivoption kann noch die maximale Größe des Archivs angegeben werden, bei der eine Durchsuchung stattfinden soll.

Mit Aktivieren automatisches Suchen kann das automatische Scannen aktiviert und mit Deaktivieren automatisches Suchen deaktiviert werden.

Email Schutz

Das Ganze kann natürlich auch in den Mailclient eingefügt werden.

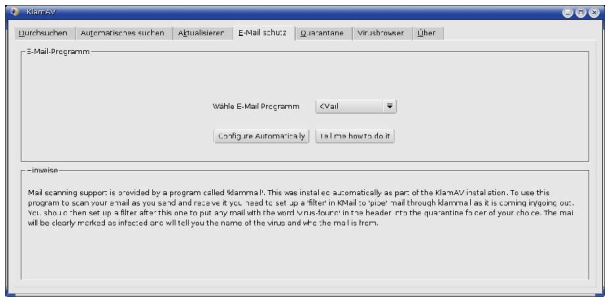


Abbildung 16: Integration in den Mailclient

Wer kmail benutzt, kann sich KlamAV durch den Schaltknopf Configure Automatically automatisch einbinden lassen. Alle Anderen müssen dies manuell machen, wobei das Prinzip bei allen das Gleiche ist. Es wird ein Filter benötigt, der die einkommenden Mails an das mitgelieferte Klammail weitereicht. Dann wird ein zweiter Filter benötigt, der die von Klammail mit einer Virusmakierung versehenen Mails in einen extra Ordner verschiebt oder gleich löscht. Die meisten Mailclients auf Linux besitzen die Möglichkeit solcher Filterregeln.

Die Quarantäne

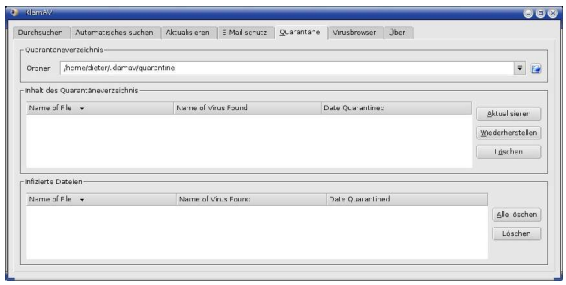


Abbildung 17: Quarantäne

Unter der Registerkarte Quarantine finden wir die Quarantäne vor. Ganz oben (Quarantäneverzeichnis) kann der Pfad zu dieser Karantäne eingestellt werden. Darauf achten, dass Schreibrechte zu diesem Pfad vorhanden sind. Im Fenster Inhalt des Quarantäneverzeichnis können die derzeit in Quarantäne liegenden Dateien betrachtet werden. Dort wird der Name der Datei, der Name des Virus und das Datum der Isolierung angezeigt.

Die Knöpfe daneben haben folgende Bedeutung:
Aktualisieren = Auffrischen und den Inhalt des Fensters aktualisieren
Wiederherstellen = die markierte Datei wird wieder an Ihren Ursprungsort zurückgeschoben.
Löschen = die markierte Datei wird endgültig gelöscht.

Durch einen Rechtsklick auf eine markierte Datei kann wieder nach der Virenbeschreibung im ClamAV Virenpool, auf Google oder bei TrendMicro gesucht werden.

Im Fenster darunter wird die History angezeigt. Dort werden die in der Vergangenheit gefundenen befallenen Dateien, die in der Quarantäne gelandet sind, aufgelistet. Hier hat man folgende Möglichkeiten:

Alles Löschen = alles bereinigen, dann werden alle Einträge gelöscht.
Löschen = der markierte Eintrag wird gelöscht.

Der Virenbrowser

Die Registerkarte Virus Browser ist eine Art Minibrowser mit dem man Details über die Viren abrufen kann (Internetverbindung vorausgesetzt). Auf der linken Seite werden alle Viren, die KlamAV bekannt sind, aufgelistet. Durch einen Doppelklick können nun Details des jeweiligen Virus abgerufen werden. Diese werden im rechten Fenster in einem Tab dargestellt. Alternativ besteht die Möglichkeit, durch einen Rechtsklick auf einen Virusnamen die Details entweder aus dem Viruspool, von TrendMicro oder von Google zu holen. In dem kleinen oberen Eingabefeld kann man nach einem Virus durch Eingeben des Namens suchen.

Abbildung 18: Virenliste

Über KlamAV

Durch die Registerkarte „About“ können Informationen über KlamAV abgerufen werden. Auch dies ist ein Browserfenster, so dass die ausgewählten Links in diesem Fenster dargestellt werden.

Weiterführende Informationen

KlamAV: http://KlamAV.sourceforge.net/
ClamAV: http://www.ClamAV.net
dazuko: http://www.dazuko.org
clamassassin: http://drivel.com/clamassassin/
ClamAV und Mandriva Linux:
http://www.mandrivauser.de/index.php?option=com_content&task=view&id=119&Itemid=47