



www.avira.de



Handbuch für Anwender

 **AntiVir[®]**
UNIX Server

Inhaltsverzeichnis

1	Über dieses Handbuch	3
1.1	Einleitung	3
1.2	Aufbau des Handbuchs	3
1.3	Zeichen und Symbole	4
1.4	Abkürzungen	5
2	Produktinformationen	7
2.1	Leistungsumfang	8
2.2	Lizenzierungskonzept	8
2.3	Funktionsweise von AntiVir	9
2.4	Systemvoraussetzungen	10
2.5	Technische Informationen	10
3	Installation	11
3.1	Installationsdateien bereitstellen	11
3.2	Lizenzierung	12
3.3	Erstellen des Kernel-Moduls Dazuko	12
3.4	Anbindung an Samba	14
3.5	AntiVir installieren	16
3.6	AntiVir erneut installieren	23
3.7	AntiVir UNIX Server über grafische Installationsroutine installieren	24
3.8	Anbindung an Produkte von Fremdherstellern	31
4	Konfiguration	33
4.1	Übersicht	33
4.2	Konfigurationsdateien	34
4.3	Konfigurationsscript	42
4.4	Konfigurieren des AntiVir Samba Scanners	43
4.5	Konfigurieren regelmäßiger Updates	46
4.6	AntiVir UNIX Server testen	52
5	Bedienung	53
5.1	AntiVir Kommandozeilenscanner im Überblick	53
5.2	AntiVir Kommandozeilenscanner in der Anwendung	58
5.3	Vorgehen bei Fund eines Virus/unerwünschten Programms	61
6	Grafische Benutzeroberfläche (GUI)	63
6.1	Übersicht	63
6.2	AntiVir Scanner	64
6.2.1	AntiVir Scanner über GUI bedienen	64
6.2.2	AntiVir Scanner über GUI konfigurieren	68
6.3	AntiVir Guard	74
6.3.1	AntiVir Guard über GUI bedienen	74
6.3.2	AntiVir Guard über GUI konfigurieren	78

7	Service	85
7.1	Support	85
7.2	Online-Shop	85
7.3	Kontakt	85
8	Anhang	87
8.1	Glossar	87
8.2	Weitere Infoquellen	88
8.3	Goldene Regeln zur Virenvorsorge	89

1 Über dieses Handbuch

In diesem Kapitel erhalten Sie einen Überblick über Aufbau und Inhalt des Handbuchs.

Nach einer kurzen Einleitung erhalten Sie Informationen zu folgenden Themen:

- [Aufbau des Handbuchs](#) – Seite 3
- [Zeichen und Symbole](#) – Seite 4

1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen zu AntiVir zusammengestellt und führen Sie Schritt für Schritt durch Installation, Konfiguration und Bedienung der Software.

Im Anhang finden Sie ein Glossar, das Ihnen grundlegende Begriffe erläutert.

Weitere Informationen und Hilfestellung bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter (siehe [Service](#) – Seite 85).

Ihr Team von Avira




1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer AntiVir-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	Inhalt
1 Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole
2 Produktinformationen	Allgemeine Hinweise zur Software AntiVir, zu Aufbau, Funktionsweise, Systemvoraussetzungen und Lizenzierung
3 Installation	Anleitung zur Installation von AntiVir UNIX Server auf Ihrem System – sowohl Skript-basiert als auch über eine grafische Installationsroutine
4 Konfiguration	Anleitung zur optimalen Anpassung von AntiVir auf Ihr System
5 Bedienung	Die Arbeit mit AntiVir, nachdem es installiert wurde; gezielte Suche nach Viren und unerwünschten Programmen; Verhalten beim Auffinden von Viren und unerwünschten Programmen
6 Grafische Benutzeroberfläche (GUI)	Allgemeine Hinweise zur GUI; Bedienung und Konfiguration von AntiVir UNIX Server über die GUI
7 Service	Support und Service von Avira GmbH
8 Anhang	Glossar mit Erläuterungen zu Fachbegriffen und Abkürzungen, Goldene Regeln zur Virenvorsorge

1.3 Zeichen und Symbole

In diesem Handbuch werden folgende Zeichen und Symbole verwendet:

Symbol	Erläuterung
✓	... steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss
▶	... steht vor einem Handlungsschritt, den Sie ausführen
↳	... steht vor einem Ergebnis, das direkt aus der vorangehenden Handlung folgt
	... steht vor einer Warnung bei Gefahr von kritischem Datenverlust oder Schäden an der Hardware
	... steht vor einem Hinweis mit besonders wichtigen Informationen, z. B. zu den folgenden Handlungsschritten
	.. steht vor einem Tipp, der das Verständnis und die Nutzung von AntiVir erleichtert.

Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

Hervorhebungen im Text	Erläuterung
Strg+Alt	Taste bzw. Tastenkombination
<code>/usr/lib/AntiVir/antivir</code>	Dateinamen und Pfadangaben
<code>ls usr/lib/AntiVir</code>	Eingaben des Anwenders
Komponente auswählen Alles Markieren	Elemente der Software-Oberfläche wie Menüpunkte, Fenstertitel, Schaltflächen in Dialogfenstern
http://www.avira.de	URLs
Zeichen und Symbole – Seite ...	Querverweise innerhalb des Dokuments

1.4 Abkürzungen

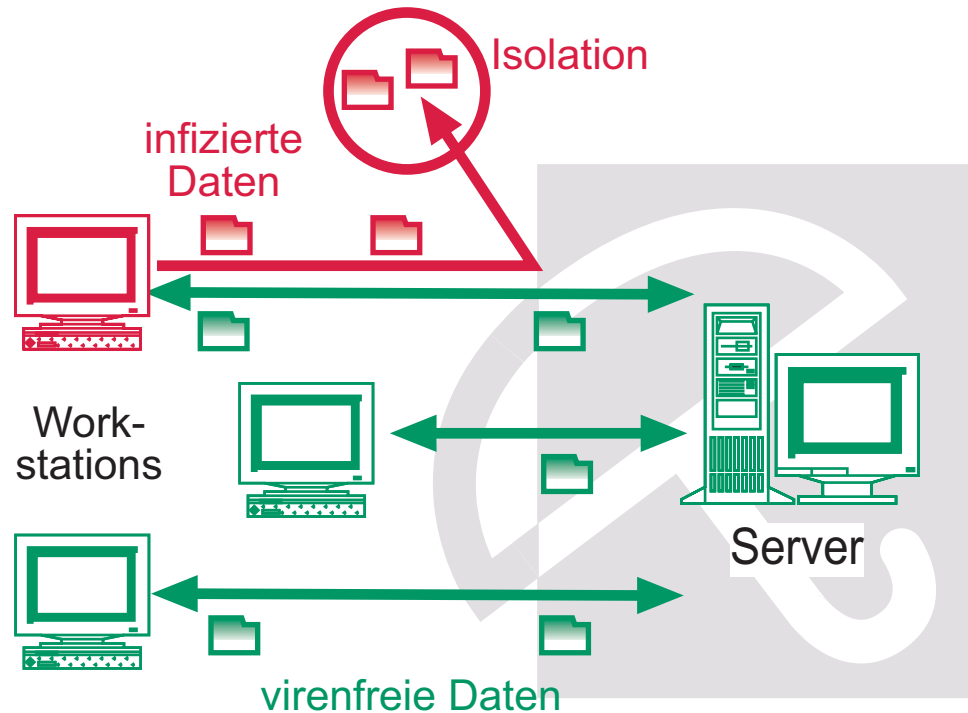
In diesem Handbuch werden folgende Abkürzungen verwendet:

Abkürzung	Erläuterung
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
GPL	General Public License
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
PMS	Possibly Malicious Software
RFC	Request For Comment
SMTP	Simple Mail Transfer Protocol
VDF	Virus Definition File

2 Produktinformationen

Sie sind zuständig für eine Vielzahl von Workstations und Servern im Netzwerk. Doch auch Sie haben nur zwei Augen.

Die Server sind das Herz des Netzwerks. Können beispielsweise Viren hier ungehindert eindringen und sich verbreiten, ist es nur ein kleiner Schritt bis zum Infarkt des Netzwerks. Hiervor schützen die Produkte von AntiVir für Server.



Immer öfter nehmen UNIX-Rechner die Funktion z. B. von File-Servern oder Email-Gateway-Servern ein. Sie transportieren und lagern also auch Daten, die nicht im direkten Zusammenhang mit UNIX stehen, z. B. Dokumente aus Office-Paketen und Email-Attachments. Viren können dann auf einem Windows-Client, der auf den Server zugreift, ungehindert ihr Zerstörungswerk ausführen.

AntiVir UNIX Server ist ein umfassendes und flexibles Werkzeug, um der Gefahr von Viren und unerwünschten Programmen auf einem Server zu begegnen und Ihr System zuverlässig zu schützen.

Zwei ganz wichtige Hinweise gleich zu Beginn:



Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen.

- Fertigen Sie grundsätzlich regelmäßig Sicherungskopien (Backups) Ihrer Daten an.



Ein Virenschutzprogramm ist nur dann zuverlässig und wirksam, wenn es aktuell ist.

- Stellen Sie die Aktualität von AntiVir über automatische Updates sicher. Sie erfahren in diesem Handbuch, was Sie hierfür tun müssen.

2.1 Leistungsumfang

AntiVir UNIX Server bietet umfangreiche Konfigurationsmöglichkeiten, damit Sie die Kontrolle über Ihr Netzwerk behalten.

Die wesentlichen Leistungsmerkmale von AntiVir UNIX Server:

- Einfache Installation durch Installationsskript sowie durch grafische Installationsroutine
- Einfache Konfiguration: Unterstützung der Konfiguration durch das Konfigurationsscript mit Hilfetexten
- Kommandozeilengestützter Scanner (On-Demand):
Konfigurierbare Suche nach allen bekannten Typen sog. "Malware" (Viren, Trojaner, Backdoor-Programme, Hoaxe, Würmer usw.)
- Residenter Wächter (On-Access):
Konfigurierbare Reaktionen auf den Fund von Viren und unerwünschten Programmen: Reparieren, Verschieben, Umbenennen von Programmen oder Dateien; automatisches Entfernen von Viren und unerwünschten Programmen
- Heuristische Makroviren-Erkennung
- Erkennt alle gebräuchlichen Archivtypen mit einstellbarer Rekursionstiefe bei verschachtelten Archiven
- Einfache Integration in automatisierte Aufgaben (Jobs) wie definierte Suchläufe zu festgelegten Zeiten
- Automatische Updates der AntiVir-Software über das Internet
- Umfassende Protokoll-, Warn- und Benachrichtigungsfunktionen für den Administrator; Versenden von Warnungen per Email (SMTP)
- Schutz vor Änderungen der Programmdateien durch intensiven Selbsttest
- Optional komfortable grafische Benutzeroberfläche (GUI) zur Bedienung und Konfiguration von AntiVir UNIX Server

2.2 Lizenzierungskonzept

Um AntiVir zu nutzen, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an
(siehe http://www.avira.com/documents/general/pdf/de/avira_eula_de.pdf).

Sie können die vielfältigen Funktionen von AntiVir mit folgenden Lizenz-Modellen nutzen:

- Demoversion
- Vollversion
- Komfortpaket

Die Lizenzierung ist abhängig von der Anzahl der Benutzer im Netzwerk, die durch AntiVir geschützt werden sollen.

Die Lizenz wird über die Lizenzdatei *hbedv.key* vergeben. Diese erhalten Sie von Avira GmbH per Email. Sie enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Sie kann also auch die Lizenz für mehrere Produkte von Avira GmbH enthalten.

Demoversion	<p>Ohne Lizenzdatei läuft die AntiVir Software als Demoversion. Dabei werden nicht alle von der lizenzierten Version erkennbaren Viren und andere unerwünschte Programme erkannt, sondern lediglich Test-Signaturen. Dieser Demo-Modus dient dazu, die Funktionsweise und die Bedienung der Software zu verdeutlichen und die Integration in eigene Abläufe zu erproben, sie leistet keinen tatsächlichen Schutz vor Malware. Ein automatisches Update ist nicht möglich, d.h. neue Virendefinitionsdateien und eine neue AntiVir Search Engine müssen immer manuell von der Webseite heruntergeladen werden.</p> <p>Es besteht keine Möglichkeit, den Zugriff auf betroffene Dateien zu sperren oder sie über AntiVir zu reparieren oder zu verschieben.</p>
Evaluation Version	<p>Nähere Informationen zur Evaluation Version erhalten Sie auf unserer Webseite http://www.avira.de.</p>
Vollversion	<p>Zum Leistungsumfang einer Vollversion gehören:</p> <ul style="list-style-type: none">• Bereitstellung der AntiVir-Version zum Download aus dem Internet• Lizenzdatei per Email zur Freischaltung von der Demoversion auf die Vollversion• Ausführliche Installationsanleitung (digital)• Bereitstellung von PDF-Handbüchern zum Download aus dem Internet• Vierwöchiger Installationssupport ab Kaufdatum• Newsletter-Service (per Email)• Update-Service auf die Programmdateien und die VDF per Internet
Komfortpaket	<p>Das Komfortpaket enthält zusätzlich zur lizenzierten Vollversion:</p> <ul style="list-style-type: none">• Alle drei Monate: Kostenlose Lieferung einer bootfähigen CD-ROM mit dem AntiVir Rescue-System und allen aktuellen AntiVir-Programmen• Umfangreiches Installationshandbuch (gedruckt) bei der Erstausslieferung• Lizenzdatei auf Diskette bei der Erstausslieferung• Newsletter-Service (gedruckt, Versand per Post)

2.3 Funktionsweise von AntiVir

Das Schutzpaket AntiVir UNIX Server besteht aus folgenden Programmteilen:

- AntiVir Kommandozeilenscanner
- AntiVir Guard
- AntiVir Samba Scanner
- Internet Updater

AntiVir Kommandozeilenscanner

... kann jederzeit aus der Kommandozeile aufgerufen werden (on Demand). Betroffene Dateien oder verdächtige Makros können über eine Vielzahl von Optionen gezielt umbenannt, repariert oder gelöscht werden. Er kann in Skripte eingebunden und von Skripten ausgewertet werden.

AntiVir Guard

... läuft im Hintergrund. Er prüft während des Zugriffs des Anwenders aus dem Netzwerk (on Access) permanent Dateien auf Viren und unerwünschte Programme. Der Zugriff auf betroffene Dateien wird sofort gesperrt. Die Dateien können automatisch umbenannt, repariert oder verschoben werden.

AntiVir Samba Scanner

... läuft im Hintergrund. Er überwacht permanent Dateien, die über den Samba Service (dedizierter Datei- und Druck-Server für Windows- und UNIX-Workstations) übertragen werden. Der Zugriff auf betroffene Dateien wird sofort gesperrt. Die Dateien können automatisch umbenannt oder verschoben werden. Eine Benachrichtigung wird – zusätzlich zum Logeintrag für den Administrator – an den entfernten Nutzer der Dateifreigabe gesendet.

Internet Updater

... stellt über Ihre Internetverbindung sicher, dass AntiVir immer auf dem neuesten Stand ist. Er prüft, ob Updates verfügbar sind, und aktualisiert ggf. Ihre Software automatisch.

2.4 Systemvoraussetzungen

AntiVir UNIX Server stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an den Server:

- Rechner mit CPU ab i386 (Linux, FreeBSD, OpenBSD, SunOS) oder PowerPC (Linux) oder Sparc (SunOS)
- 80-100 MB freier Speicherplatz auf der Festplatte
- 20 MB temporärer Speicherplatz auf der Festplatte
- 192 MB (512 MB unter SunOS) freier Hauptspeicher
- Linux mit glibc oder libc5, FreeBSD, OpenBSD oder SunOS
- bei Einsatz des on access scanners: Linux Kernel 2.2, 2.4 oder 2.6, optional mit RSBAC; FreeBSD 4, 5 oder 6; SunOS 5.7, 5.8, 5.9 oder 5.10 (Sparc) oder 5.9 (i386)
- bei Einsatz des AntiVir Samba Scanners: Samba-Version mit Unterstützung für den VFS-Mechanismus (ab Version 2.2.0) und samba-vscan ab Version 0.3.5
- wenn Sie die GUI verwenden wollen: Sun Java 1.4.0 oder höher

2.5 Technische Informationen

Der AntiVir Guard basiert auf Dazuko (<http://www.dazuko.org>), einem Open-Source-Softwareprojekt. Dazuko ist ein Kernel-Modul, das die Dateizugriffe an den AntiVir-Guard-Dämon weiterleitet.

Der AntiVir Samba Scanner basiert auf samba-vscan (<http://www.openantivirus.org/projects.php>), einem Open-Source-Softwareprojekt. samba-vscan ist ein VFS Plugin für Samba und besitzt ein so genanntes AntiVir Backend, das die Dateizugriffe an den AntiVir Samba Scanner weiterleitet.

Beachten Sie auch die Lizenzinformationen im Installationsverzeichnis unter */legal*.

3 Installation

Die aktuelle Version von AntiVir UNIX Server ist im Internet verfügbar. Wenn Sie im Rahmen des Komfortpakets eine AntiVir-CD-ROM besitzen, können Sie die Dateien auch von dieser installieren.

AntiVir wird als gepacktes Archiv zur Verfügung gestellt. Dieses Archiv enthält den AntiVir Guard, den AntiVir Kommandozeilenscanner und den Internet Updater.

Sie werden Schritt für Schritt durch die Installation geführt. Dieses Kapitel ist untergliedert in folgende Abschnitte:

- [Installationsdateien bereitstellen](#) – Seite 11
- [Lizenzierung](#) – Seite 12
- [Erstellen des Kernel-Moduls Dazuko](#) – Seite 12
- [Anbindung an Samba](#) – Seite 14
- [AntiVir installieren](#) – Seite 16
- [AntiVir erneut installieren](#) – Seite 23
- [AntiVir UNIX Server über grafische Installationsroutine installieren](#) – Seite 24
- [Anbindung an Produkte von Fremdherstellern](#) – Seite 31

3.1 Installationsdateien bereitstellen

Programmdatei aus dem Internet laden

- ▶ Laden Sie die aktuelle Datei von unserer Webseite <http://www.avira.de> auf Ihren lokalen Rechner. Zurzeit heißt diese Datei *antivir-server-prof-<version>.tar.gz* (ohne grafische Installationsroutine) bzw. *antivir-server-linux-gui_installer.tar.gz* (mit grafischer Installationsroutine).
- ▶ Legen Sie die Datei in einem Verzeichnis Ihrer Wahl auf dem Computer ab, auf dem AntiVir UNIX Server laufen soll, z. B. unter */tmp*.

Programmdatei von CD-ROM laden

- ▶ Wählen Sie auf Ihrer CD-ROM den Ordner */DE/PRODUCTS/UNIX/SERVER* bzw. */DE/PRODUCTS/UNIX/GUI_INSTALLERS/*.
- ▶ Kopieren Sie die Datei *antivir-server-prof-<version>.tar.gz* bzw. *antivir-server-linux-gui_installer.tar.gz* in ein Verzeichnis, z. B. nach */tmp*.

Programmdatei entpacken

Beispielhaft wird das Entpacken der Datei ohne grafische Installationsroutine beschrieben.

- ▶ Wechseln Sie in das temporäre Verzeichnis:
`cd /tmp`
- ▶ Entpacken Sie die Archivdatei für das AntiVir-Paket:
`tar xzvf antivir-server-prof-<version>.tar.gz`
 - ↳ Ein Verzeichnis *antivir-server-prof-<version>* wird im temporären Verzeichnis angelegt.

- ▶ Wechseln Sie in folgendes Verzeichnis:
`cd /tmp/antivir-server-prof-<version>/contrib/dazuko`
- ▶ Entpacken Sie die Archivdatei für das Kernel-Modul Dazuko:
`tar xzvf dazuko-<version>.tar.gz`
 - ↳ Ein Ordner *dazuko-<version>* wird angelegt.

3.2 Lizenzierung

Sie müssen AntiVir lizenzieren, um es in vollem Umfang nutzen zu können (siehe [Lizenzierungskonzept](#) – Seite 8). Hierfür benötigen Sie eine Lizenzdatei *hbedv.key*. Diese Lizenzdatei enthält Informationen zu Umfang und Dauer der Lizenz. Ohne Lizenzdatei läuft AntiVir ausschließlich als Demoversion mit reduziertem Leistungsumfang.

Lizenz erwerben

- ▶ Kontaktieren Sie uns telefonisch oder per Email (info@avira.de), um eine gültige Lizenzdatei für AntiVir zu erhalten.
 - ↳ Sie erhalten eine Lizenzdatei per Email zugesandt.
- ▶ Sie können AntiVir auch einfach und schnell über unseren Online-Shop erwerben (weitere Informationen siehe <http://www.avira.de>).

Lizenzdatei einspielen

- ▶ Kopieren Sie die Lizenzdatei *hbedv.key* von Diskette oder Email in Ihr Installationsverzeichnis */tmp/antivir-server-prof-<version>*.



Sie können die Installation auch ohne Lizenzdatei durchführen. AntiVir läuft dann als Demoversion. Die Lizenzdatei kann nachträglich in das AntiVir-Programmverzeichnis */usr/lib/AntiVir* kopiert werden.

3.3 Erstellen des Kernel-Moduls Dazuko

Das Kernel-Modul Dazuko ist auf allen Plattformen erforderlich, wenn die Funktionalität des AntiVir Guard benutzt werden soll.

Das Kernel-Modul Dazuko ist erforderlich, um den residenten Wächter AntiVir Guard einzusetzen.



Es ist möglich, AntiVir zunächst ohne Kernel-Modul Dazuko zu installieren. In diesem Fall läuft AntiVir ohne den AntiVir Guard. Lesen Sie hierfür weiter in [AntiVir ohne den AntiVir Guard installieren](#) – Seite 16.

Das Modul müssen Sie selber kompilieren, denn Ihrem UNIX-Kernel und Dazuko müssen die gleichen Quelldateien zugrunde liegen. Nur so ist sichergestellt, dass Dazuko auf die gleichen Systemfunktionen wie der UNIX-Kernel zugreifen kann.



Wenn der Lieferant Ihrer Distribution bereits ein exakt zu Ihrem Kernel passendes Modul beigelegt hat:

- ▶ Überspringen Sie den nachfolgend beschriebenen Schritt.
- ▶ Stellen Sie fest, unter welchem Namen das Modul auf der Festplatte gespeichert wurde (bei der späteren Installation des AntiVir Guard wird diese Information benötigt). Verwenden Sie dafür z. B. den folgenden Befehl:

```
find /lib/modules/`uname -r` -name 'dazuko*'
```



Das Installationspaket enthält für SunOS (Sparc und i386) ein binäres Modul, so dass Sie dieses auf dieser Plattform nicht selbst erstellen müssen.

Im Folgenden wird das Vorgehen so beschrieben, dass Sie auch ohne Expertenkenntnisse zum Ziel kommen. Dennoch sind Kenntnisse in der Kompilierung des UNIX-Kernels nützlich, insbesondere wenn Fehler auftreten. Weitere Informationen hierzu erhalten Sie unter <http://www.tldp.org/HOWTO/Kernel-HOWTO.html>

Dazuko kompilieren

- ✓ Stellen Sie sicher, dass sich der Quellcode für den UNIX-Kernel in `/usr/src/linux` befindet. Falls nicht, installieren Sie ihn nach. Informationen dazu finden Sie in der Dokumentation Ihrer UNIX-Distribution.
- ✓ Stellen Sie sicher, dass sich die Programme zur Kompilierung eines Kernels (z. B. gcc) auf Ihrem Rechner befinden. Bei einer UNIX-Standardinstallation ist dies der Fall. Falls nicht, installieren Sie die benötigten Programmpakete nach. Informationen dazu finden Sie in der Dokumentation Ihrer UNIX-Distribution.
- ✓ Ihr UNIX-Kernel muss auf dem Quellcode in `/usr/src/linux` basieren. In den meisten Fällen, insbesondere nach einer Neuinstallation von UNIX, sollte dies der Fall sein. Absolute Sicherheit hierüber können Sie allerdings nur gewinnen, indem Sie den auf dem Computer eingesetzten Kernel aus genau diesen Quellen neu kompilieren.



Bei Unsicherheiten über den Stand Ihres UNIX-Kernels können Sie dennoch die Installation fortführen. Schlimmstenfalls gelingt später zur Laufzeit die Integration von Dazuko in Ihren UNIX-Kernel nicht, so dass der Start des AntiVir Guard fehlschlägt. In diesem Fall erhalten Sie eine entsprechende Meldung und können die Situation danach bereinigen.

- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie Dazuko entpackt haben, also z. B.:

```
cd /tmp/antivir-server-prof-<version>/contrib/dazuko-<version>
```
- ▶ Lassen Sie das Skript *configure* die Konfiguration Ihres Rechners überprüfen und unter Einbeziehung vorgefundener Details eine entsprechende Anleitung zur weiteren Übersetzung der Software erstellen:

```
./configure
```

- ▶ Kompilieren Sie Dazuko mit:
`make`
- ▶ Optional: Prüfen Sie, ob das gerade erstellte Modul mit dem auf dem Rechner laufenden Kernel zusammenarbeitet:
`make test`
 - ↳ Sie erhalten je nach verwendetem Betriebssystem eine Datei *dazuko.o* oder *dazuko.ko* im temporären Verzeichnis. Die Pfadangabe zu dieser Datei wird später vom AntiVir-Installationsskript benötigt

Weitere aktuelle Informationen zu Dazuko erhalten Sie auf der Webseite <http://www.dazuko.org>. Distributionsspezifische Details sind oft schon in den FAQ ausgeführt.

3.4 Anbindung an Samba

Das AntiVir Backend für samba-vscan ist auf allen Plattformen erforderlich, um die Funktionalität des AntiVir Samba Scanners zu nutzen.

Das AntiVir Backend für samba-vscan ist erforderlich, um transparent alle Dateizugriffe über den Samba Service zu überwachen.



Es ist möglich, AntiVir zunächst ohne samba-vscan zu installieren. In diesem Fall läuft AntiVir ohne den AntiVir Samba Scanner. Der entsprechende Schutz der Dateifreigaben kann auch mit dem AntiVir Guard erreicht werden. Allerdings sind dann die Benachrichtigungen an den entfernten Nutzer der Dateifreigabe über die Option `ExternalProgram` von AntiVir Guard und selbst erstellte Logik zu implementieren (z. B. über UNIX-Scripts).

Das AntiVir Backend für samba-vscan (realisiert durch ein VFS Plugin für Samba) müssen Sie selbst erstellen, denn Ihrem Samba Service und dem Backend müssen die gleichen Quellen zugrunde liegen. Nur so ist die korrekte Funktion des VFS Plugin und die Stabilität Ihres Datei-Servers sichergestellt.



Wenn der Lieferant Ihrer Distribution bereits ein exakt zu Ihrem Samba Service passendes AntiVir Backend beigelegt hat:

- ▶ Überspringen Sie den nachfolgend beschriebenen Schritt.
- ▶ Stellen Sie fest, unter welchem Namen das Backend und eine passende Konfigurationsdatei auf der Festplatte gespeichert wurden. Verwenden Sie dafür z. B. die folgenden Befehle:
`find /usr -name 'vscan-antivir.so'`
`find /usr -name 'vscan-antivir.conf*'`

Im Folgenden werden Kenntnisse über die Kompilierung von Samba und samba-vscan vorausgesetzt. Entsprechende Anleitungen finden Sie in der Dokumentation der Quellpakete und auf den Webseiten der entsprechenden Projekte.

Samba vorbereiten

- ✓ Stellen Sie sicher, dass sich die Programme zur Kompilierung der Quellen (z. B. gcc, make) auf Ihrem Rechner befinden. Bei einer UNIX-Standard-Installation ist dies

meist der Fall. Falls nicht, installieren Sie die benötigten Programmpakete nachträglich. Informationen dazu finden Sie in der Dokumentation Ihrer UNIX-Distribution.

- ✓ Stellen Sie sicher, dass Sie den Quelltext von `samba-vscan` in der Version 0.3.5 oder neuer verfügbar haben. Für Version 0.3.5 liegt ein Patch vor, der das AntiVir Backend implementiert. Ab Version 0.3.6 von `samba-vscan` ist das AntiVir Backend bereits enthalten.
- ✓ Stellen Sie sicher, dass Sie den Quelltext von Samba in exakt der Version verfügbar haben, die Sie als Datei-Server einsetzen. Sie müssen Samba nicht vollständig aus diesen Quellen übersetzen und installieren, die Quellen und ihre Konfiguration werden aber vom `samba-vscan`-Paket benötigt. Natürlich können Sie mit der Installation des selbst übersetzten Samba am besten sicherstellen, dass Service und VFS Plugin korrekt zueinander passen.
- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie Samba entpackt haben, z. B.:

```
cd /tmp
gunzip < samba-<version>tar.gz | tar xf -
cd samba-<version>/source
```
- ▶ Lassen Sie das `configure`-Script die Konfiguration Ihres Rechners prüfen und unter Einbeziehung vorgefundener Details eine entsprechende Anleitung zur weiteren Übersetzung der Software erstellen:

```
./configure
```
- ▶ Erstellen Sie die von `samba-vscan` benötigten Zusatzinformationen:

```
make proto
```
- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie `samba-vscan` entpackt haben, z. B.:

```
cd /tmp
bunzip2 < samba-vscan-0.3.5.tar.bz2 | tar xf -
cd samba-vscan-0.3.5
```
- ▶ Entpacken Sie das Archiv mit dem AntiVir Backend für `samba-vscan`. Es enthält die AntiVir-spezifischen Quellen sowie einen Patch, der auf `samba-vscan` 0.3.5 aufsetzt und das AntiVir Backend einbindet. Bringen Sie den Patch an (ab Version 0.3.6 von `samba-vscan` ist dieser Schritt nicht mehr nötig, da das AntiVir Backend bereits enthalten ist).

```
gunzip < /tmp/samba-vscan-antivir-0.3.5.tar.gz |
tar xf -
patch -p0 < patch-sambavscan-hookup.diff
```
- ▶ Konfigurieren und übersetzen Sie `samba-vscan`. Dabei müssen Sie angeben, wo die Samba-Quellen (s. o.) zu finden sind:

```
./configure --with-samba-source=/tmp/samba-<version>/
source
make
make install
```
- ▶ Eine Beispiel-Konfiguration für das AntiVir `samba-vscan` Backend wird mitgeliefert, die Sie als Vorlage für eigene Anpassungen verwenden können:

```
cp antivir/vscan-antivir.conf /usr/local/samba/lib
```

Für den Einsatz des AntiVir Samba Scanners ist in der Datei `smb.conf` für die Dateifreigaben, die überwacht werden sollen, das `vscan-antivir.so`-Plugin zu aktivieren (siehe Kapitel [Konfigurieren des AntiVir Samba Scanners](#) – Seite 43). Neben Samba muss kein zusätzlicher Scan-Service gestartet werden, das `vscan-antivir.so` Plugin handhabt diesen Aspekt selbst.

3.5 AntiVir installieren

Die Installation von AntiVir läuft weitgehend automatisch über ein Installationsskript ab. Dieses Skript führt folgende Aufgaben durch:

- Prüfen der Installationsdateien auf Vollständigkeit
- Prüfen, ob Sie ausreichende Rechte zur Installation besitzen
- Prüfen, inwieweit schon eine Version von AntiVir auf dem Rechner vorhanden ist
- Kopieren der Programmdateien. Bereits vorhandene veraltete Dateien werden überschrieben.
- Kopieren der AntiVir-Konfigurationsdateien. Bereits vorhandene AntiVir-Konfigurationsdateien werden beibehalten.
- Optional Erstellen eines Links in `/usr/bin`, so dass AntiVir aus allen Verzeichnissen ohne vorangestellte Pfadangabe aufgerufen werden kann.
- Optional Installieren des Update Daemons und des residenten Wächters AntiVir Guard.
- Optional Konfigurieren eines automatischen Starts des Internet Updater und des AntiVir Guard beim Systemstart.
- Folgende Schritte sind für die Erstinstallation erforderlich: [Installation vorbereiten](#) – Seite 16
- Wenn Dazuko noch nicht kompiliert wurde: [AntiVir ohne den AntiVir Guard installieren](#) – Seite 16
- Wenn Dazuko bereits kompiliert wurde: [AntiVir mit dem AntiVir Guard installieren](#) – Seite 19

Installation vorbereiten

- Loggen Sie sich ein als **root**. Ansonsten haben Sie keine ausreichende Berechtigung für die Installation und das Skript bricht mit einer Fehlermeldung ab.
- Wechseln Sie in das Verzeichnis, in das Sie AntiVir entpackt haben, also etwa:
`cd /tmp/antivir-server-prof-<version>`

AntiVir ohne den AntiVir Guard installieren

Wenn Sie noch kein Kernel-Modul Dazuko kompiliert haben, müssen Sie AntiVir zunächst ohne den AntiVir Guard installieren. Der AntiVir Guard kann später problemlos nachinstalliert werden.

- Geben Sie ein:
`./install`
Achten Sie auf den führenden Punkt und Schrägstrich. Ein Aufruf von "install" ohne diese Pfadangabe führt typischerweise zum Aufruf eines anderen, hier nicht zu involvierenden Kommandos und in der Folge zu Fehlermeldungen oder ungewollten Aktivitäten. Der für den Lizenztext verwendete Dateibetrachter kann typischerweise mit der Taste 'q' verlassen werden.

- ↳ Das Installationsskript läuft an. Nach dem Akzeptieren der Lizenzbedingungen werden die Programmdateien kopiert. Optional übernimmt der Installer einen zuvor bereitgelegten Lizenzkey:

```
Do you agree to the license terms? [n] y
creating /usr/lib/AntiVir ... done
1) installing command line scanner
copying bin/antivir to /usr/lib/AntiVir/ ... done
copying vdf/antivir0.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir1.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir2.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir3.vdf to /usr/lib/AntiVir/ ... done

Enter the path to your key file: [hbedv.key]
copying hbedv.key to /usr/lib/AntiVir/hbedv.key ... done
copying script/configantivir to /usr/lib/AntiVir/ ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir ... done
installation of command line scanner complete
```

- ↳ Anschließend werden Sie gefragt, ob der Internet Update Daemon installiert werden soll:

```
2) installing automatic internet update daemon
An internet update daemon is available ...
...
Would you like to install the automatic internet update daemon? [n]
```



Der Internet Update Daemon ist nicht notwendig, um Updates zu erhalten. Sie können jederzeit mit AntiVir ein manuelles Update über das Internet starten. Hinweise hierzu unter [AntiVir manuell aktualisieren](#) – Seite 60

Für die Erstinstallation wird aber eine Installation des Internet Update Daemons empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren.

Installation mit
Update
Daemon

Wenn Sie den Internet Update Daemon installieren wollen (empfohlen):

- Geben Sie Y ein und bestätigen Sie mit Enter.

- ↳ Der Internet Update Daemon wird installiert. Anschließend werden Sie gefragt, ob der Daemon beim Systemstart automatisch gestartet werden soll:

```
Would you like to install the internet update daemon? [n] y
copying script/rc.avupdater.SuSE8x to /usr/lib/AntiVir/avupdater ... done
checking for existing /etc/avupdater.conf ... not found
copying etc/avupdater.conf to /etc/ ... done

Would you like the internet update daemon to start automatically? [y]
```

- Bestätigen Sie mit Enter. Sie können diese Einstellung später wieder rückgängig machen.

↳ Der automatische Systemstart wird konfiguriert:

```
setting up startup script ... done
installation of the internet update daemon complete
```

Installation
ohne Update
Daemon

Wenn Sie den Internet Update Daemon später oder gar nicht installieren wollen:

- ▶ Geben Sie N ein und drücken Sie Enter.
- ▶ Bestätigen Sie mit Enter.

AntiVir Guard
abwählen

Anschließend wird gefragt, ob der AntiVir Guard installiert werden soll:

```
3) installing AvGuard
Version 2.1.8-30 of AntiVir for UNIX Server is capable of on-access,
real-time scanning of files. This provides
...
There are several ways in which you can install AvGuard.
    module - Dazuko will be loaded by the avguard script
    kernel  - Dazuko is always loaded
              (and should not be loaded by the avguard script)
    no install - do not install AvGuard at this time
...
available options: m k n
How should AvGuard be installed? [k]
```

- ▶ Geben Sie N ein und bestätigen Sie mit Enter.

GUI
installieren

Anschließend wird gefragt, ob AntiVir mit der optionalen grafischen Benutzeroberfläche (GUI) installiert werden soll:

```
4) installing GUI (+ SMC support)
...
Would you like to install the GUI (+ SMC support)? [y]
```



AntiVir UNIX Server wird mit einer GUI bereit gestellt, die es ermöglicht, die Echtzeit-Aktivitäten zu überwachen, Logeinträge anzuzeigen und das Produkt zu konfigurieren. AntiVir ist aber auch ohne GUI voll funktionsfähig.

Wenn Sie die GUI installieren wollen:

- ✓ Java 1.4.0 oder höher muss auf dem Rechner installiert sein
- ▶ Geben Sie auf die Frage nach der GUI-Installation Y ein.
 - ↳ Die Programmdateien für die GUI werden kopiert.

Konfiguration starten Schließlich haben Sie die Möglichkeit, den AntiVir Updater zu konfigurieren und AntiVir Guard sofort zu starten (falls zuvor in der Installation aktiviert, startet AntiVir Guard automatisch beim Booten):

```
5) configuring AntiVir Updater
...
Would you like to configure AntiVir updater now? [y] n
Would you like to start AvGuard now? [y] n
```



Wenn Sie hier mit Y bestätigen, wird das Konfigurationsskript für AntiVir gestartet. Die Konfiguration können Sie auch später jederzeit durchführen. Wir empfehlen, sich hierfür zunächst mit den Möglichkeiten der Konfiguration vertraut zu machen und die Konfiguration später durchzuführen.

- Brechen Sie mit N ab.
 - ↳ Sie erhalten abschließend die Bestätigung, dass die Installation erfolgreich verlaufen ist:

```
Installation of the following features complete:
AntiVir command line scanner
AntiVir Internet Update Daemon
AntiVir GUI

Note: It is highly recommended that you perform an update now to
ensure up-to-date protection. This can be done by running:

antivir --update

Be sure to read the README file for additional information.
Thank you for your interest in AntiVir for UNIX Server.
```

AntiVir mit dem AntiVir Guard installieren

- ✓ Stellen Sie sicher, dass das Kernel-Modul Dazuko bereits kompiliert ist (siehe [Erstellen des Kernel-Moduls Dazuko](#) – Seite 12).
- Geben Sie ein:


```
./install
```

Achten Sie auf den führenden Punkt und Schrägstrich. Ein Aufruf von "install" ohne diese Pfadangabe führt typischerweise zum Aufruf eines anderen, hier nicht zu involvierenden Kommandos und in der Folge zu Fehlermeldungen oder ungewollten Aktivitäten. Der für den Lizenztext verwendete Dateibetrachter kann typischerweise mit der Taste 'q' verlassen werden.

- ↳ Das Installationsskript läuft an. Nach dem Akzeptieren der Lizenzbedingungen werden die Programmdateien kopiert. Optional übernimmt der Installer einen zuvor bereitgelegten Lizenzkey:

```
Do you agree to the license terms? [n] y
creating /usr/lib/AntiVir ... done
1) installing command line scanner
copying bin/antivir to /usr/lib/AntiVir/ ... done
copying vdf/antivir0.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir1.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir2.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir3.vdf to /usr/lib/AntiVir/ ... done

Enter the path to your key file: [hbedv.key]
copying hbedv.key to /usr/lib/AntiVir/hbedv.key ... done
copying script/configantivir to /usr/lib/AntiVir/ ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir ... done
installation of command line scanner complete
```

- ↳ Anschließend werden Sie gefragt, ob der Internet Update Daemon installiert werden soll:

```
2) installing automatic internet update daemon
An internet update daemon is available ...
...
Would you like to install the automatic internet update daemon? [n]
```



Der Internet Update Daemon ist nicht notwendig, um Updates zu erhalten. Sie können jederzeit mit AntiVir ein manuelles Update über das Internet starten. Hinweise hierzu unter [AntiVir manuell aktualisieren](#) – Seite 60

Für die Erstinstallation wird aber eine Installation des Internet Update Daemons empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren.

Installation mit
Update
Daemon

Wenn Sie den Internet Update Daemon installieren wollen (empfohlen):

- ▶ Geben Sie Y ein und bestätigen Sie mit Enter.
 - ↳ Der Internet Update Daemon wird installiert. Anschließend werden Sie gefragt, ob der Daemon beim Systemstart automatisch gestartet werden soll:

```
Would you like to install the internet update daemon? [n] y
copying script/rc.avupdater.SuSE8x to /usr/lib/AntiVir/avupdater ... done
checking for existing /etc/avupdater.conf ... not found
copying etc/avupdater.conf to /etc/ ... done

Would you like the internet update daemon to start automatically? [y]
```

- ▶ Bestätigen Sie mit Enter. Sie können diese Einstellung später wieder rückgängig machen.

↳ Der automatische Systemstart wird konfiguriert:

```
setting up startup script ... done
installation of the internet update daemon complete
```

Installation
ohne Update
Daemon

Wenn Sie den Internet Update Daemon später oder gar nicht installieren wollen:

- ▶ Geben Sie N ein und drücken Sie Enter.
- ▶ Bestätigen Sie mit Enter.

AntiVir Guard
installieren

Anschließend wird gefragt, ob der AntiVir Guard installiert werden soll:

```
3) installing AvGuard
Version 2.1.8-30 of AntiVir for UNIX Server is capable of on-access,
real-time scanning of files. This provides
...
There are several ways in which you
can install AvGuard.

      module - Dazuko will be loaded by the avguard script
      kernel  - Dazuko is always loaded
                (and should not be loaded by the avguard script)
      no install - do not install AvGuard at this time

...
available options: m k n
How should AvGuard be installed? [k]
```

- ▶ Geben Sie M ein und bestätigen Sie mit Enter.
 - ↳ Sie werden nach dem Pfad zum kompilierten Dazuko-Modul *dazuko.ko* (bzw. *dazuko.o*) gefragt:

```
Enter the full path to dazuko.ko:
```

- ▶ Geben Sie den vollständigen Pfad ein.
Beispiel: Wenn *dazuko.ko* in */tmp/antivir-server-prof-<version>/contrib/dazuko-<version>/* liegt, geben Sie ein:
/tmp/antivir-server-prof-<version>/contrib/dazuko-<version>/dazuko.ko
- ↳ Das Installationsskript übernimmt das vorgegebene Kernel-Modul und kopiert anschließend die Dateien für den AntiVir Guard.

```
detecting kernel version ... linux26-2.6.5-7.97-smp
creating /usr/lib/AntiVir/linux26-2.6.5-7.97-smp ... done
copying /tmp/antivir-server-prof-2.1.8-30/contrib/dazuko/dazuko-2.3.1/
dazuko.ko to /usr/lib/AntiVir/linux26-2.6.5-7.97-smp/dazuko.ko ... done
copying doc/avserver_de.pdf to /usr/lib/AntiVir/ ... done
copying script/rc.avguard.SuSE8x to /usr/lib/AntiVir/avguard ... done
copying doc/MANUAL to /usr/lib/AntiVir/MANUAL.avguard ... done
```

Wenn das Installationsskript Probleme zu Dazuko meldet, müssen Sie möglicherweise Ihren UNIX-Kernel neu kompilieren. Hinweise hierzu finden Sie unter <http://www.dazuko.org>

Anschließend werden Sie gefragt, ob der AntiVir Guard beim Systemstart automatisch gestartet werden soll:

Would you like AvGuard to start automatically? [y]

► Bestätigen Sie mit Enter.

↳ Im Anschluß wird der AntiVir Guard mit dem startup Script verlinkt und die Installation des AntiVir Guard abgeschlossen.

setting up startup script ... done
installation of AvGuard complete

GUI
installieren

Anschließend wird gefragt, ob AntiVir mit der optionalen grafischen Benutzeroberfläche (GUI) installiert werden soll:

4) installing GUI (+ SMC support)
...
Would you like to install the GUI (+ SMC support)? [y]



AntiVir UNIX Server wird mit einer GUI bereit gestellt, die es ermöglicht, die Echtzeit-Aktivitäten zu überwachen, Logeinträge anzuzeigen und das Produkt zu konfigurieren. AntiVir ist aber auch ohne GUI voll funktionsfähig.

Wenn Sie die GUI installieren wollen:

✓ Java 1.4.0 oder höher muss auf dem Rechner installiert sein

► Geben Sie auf die Frage nach der GUI-Installation Y ein.

↳ Die Programmdateien für die GUI werden kopiert.

Konfiguration
starten

Schließlich haben Sie die Möglichkeit, den AntiVir Updater zu konfigurieren und AntiVir Guard sofort zu starten (falls zuvor in der Installation aktiviert, startet AntiVir Guard automatisch beim Booten):

5) configuring AntiVir Updater
...
Would you like to configure AntiVir updater now? [y] n
Would you like to start AvGuard now? [y] n



Wenn Sie hier mit Y bestätigen, wird das Konfigurationsskript für AntiVir gestartet. Die Konfiguration können Sie auch später jederzeit durchführen. Wir empfehlen, sich hierfür zunächst mit den Möglichkeiten der Konfiguration vertraut zu machen und die Konfiguration später durchzuführen.

► Brechen Sie mit N ab.

- ↳ Sie erhalten abschließend die Bestätigung, dass die Installation erfolgreich verlaufen ist:

Installation of the following features complete:

AntiVir command line scanner
 AntiVir Internet Update Daemon
 AntiVir Guard
 AntiVir GUI

Note: It is highly recommended that you perform an update now to ensure up-to-date protection. This can be done by running:

`antivir --update`

Be sure to read the README file for additional information.

Thank you for your interest in AntiVir for UNIX Server.

3.6 AntiVir erneut installieren

Sie können das Installationsskript jederzeit neu aufrufen. Hiermit sind folgende Vorgänge möglich:

- Installation einer neuen Version (Upgrade). Das Installationsskript prüft die bestehende Version und installiert notwendige neue Komponenten. Einstellungen, die Sie in den Konfigurationsdateien vorgenommen haben (siehe [Konfiguration](#) – Seite 33), werden dabei nicht überschrieben, sondern übernommen.
- Nachinstallation einzelner Komponenten, z. B. des AntiVir Guard oder des Internet Update Daemons.
- Aktivierung oder Deaktivierung des automatischen Starts des Internet Update Daemons und des AntiVir Guard.

AntiVir erneut installieren

Das Vorgehen ist für alle Fälle gleich:

- ✓ Stellen Sie sicher, dass der AntiVir Guard nicht läuft:
`/usr/lib/AntiVir/avguard stop`
- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie AntiVir entpackt haben, also etwa:
`cd /tmp/antivir-server-prof-<version>`
- ▶ Geben Sie ein:
`./install`
 - ↳ Das Installationsskript läuft weitgehend ab wie in der Erstinstallation beschrieben (siehe [AntiVir installieren](#) – Seite 16).
- ▶ Ändern Sie die entsprechenden Einstellungen während der Installation.
 - ↳ AntiVir ist mit den neuen Einstellungen installiert.

3.7 AntiVir UNIX Server über grafische Installationsroutine installieren

Sie können AntiVir auch komfortabel über eine grafische Installationsroutine installieren. Dafür müssen Sie die entsprechende Datei heruntergeladen haben, wie im Kapitel [Installationsdateien bereitstellen](#) – Seite 11 beschrieben.

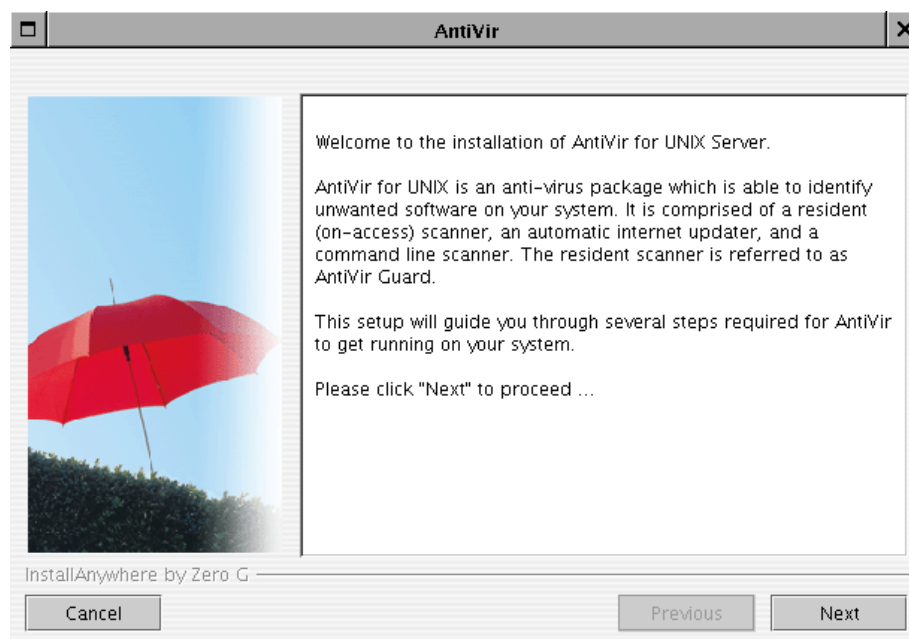


Die grafische Installationsroutine dient nur der Installation. Sie steht in keinem Zusammenhang mit der GUI, über die AntiVir UNIX Server bedient und konfiguriert werden kann.

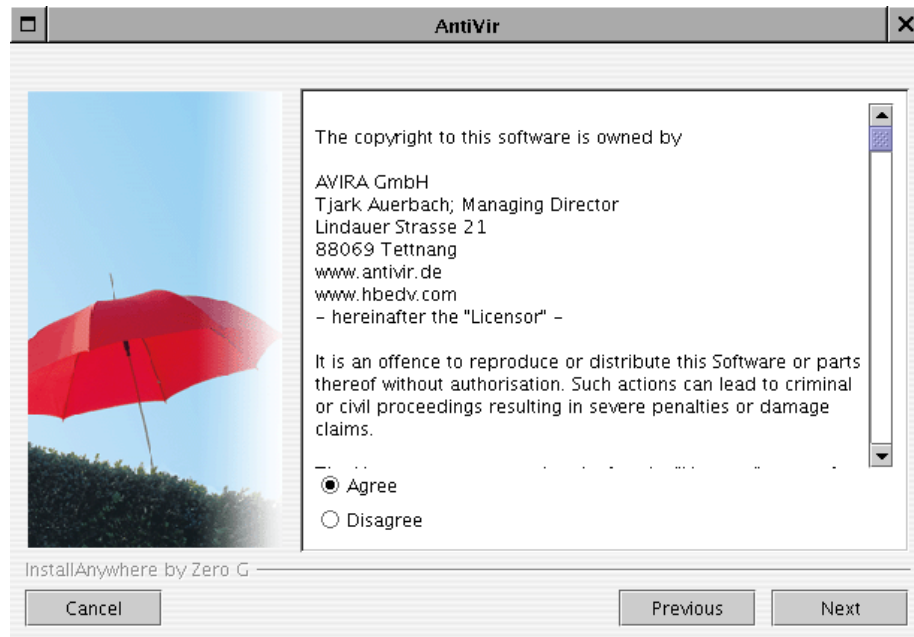


AntiVir UNIX Server mit grafischer Installationsroutine ist nur für Linux verfügbar. Es wird Java 1.4.0 oder höher benötigt.

- ✓ Die Programmdatei wurde entpackt und liegt im Verzeichnis `/tmp/antivir-server-linux-gui_installer`.
- ▶ Geben Sie ein:
`./install`
 - ↳ Es erscheint der Begrüßungstext und eine kurze Beschreibung des Programms:



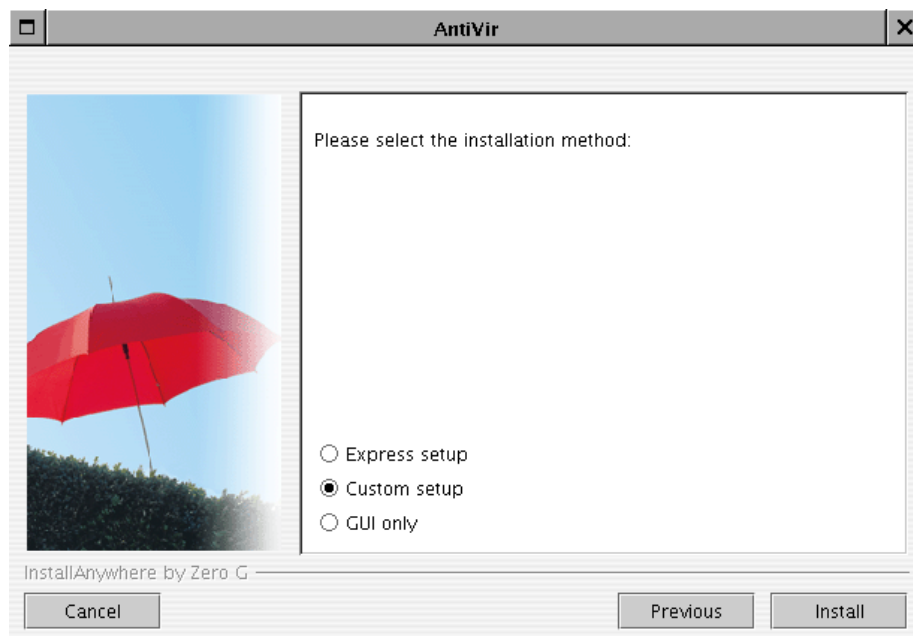
- ▶ Klicken Sie auf **Next**.
 - ↳ Das folgende Dialogfenster mit den Lizenzbedingungen erscheint:



Um die Installation fortzusetzen, müssen Sie die Lizenzbedingungen akzeptieren. Wenn **Disagree** aktiviert ist, kann die Installation nicht fortgesetzt werden.

► Aktivieren Sie die Option **Agree** und bestätigen Sie mit **Next**.

↳ Das folgende Dialogfenster erscheint:



Sie haben drei Möglichkeiten, AntiVir UNIX Server zu installieren:

- **Express setup:** Das Programm wird mit einer vorgegebenen Grundeinstellung installiert.
- **Custom setup:** Das Programm wird benutzerdefiniert installiert.
- **GUI only:** Es wird nur die GUI im Verzeichnis `usr/lib/AntiVir` installiert.

Express setup

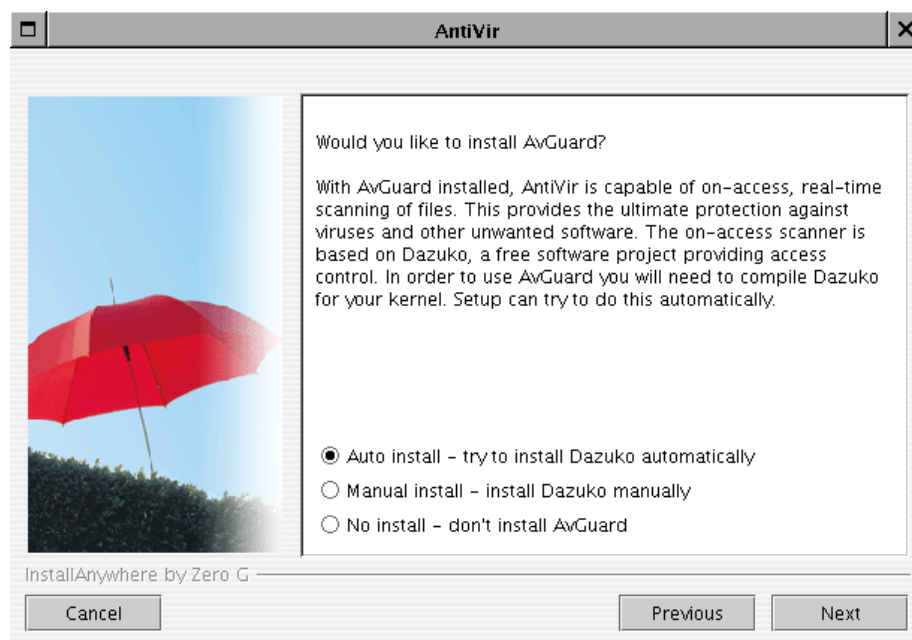
Das Programm wird mit folgender Grundeinstellung installiert:

- AntiVir UNIX Server wird in folgendes Verzeichnis installiert:
/usr/lib/AntiVir
 - Es wird der AntiVir Guard (on-access scanner) installiert.
 - Es wird kein automatischer Internet Update Daemon installiert.
 - Die GUI-Unterstützung ist aktiviert.
 - Der AntiVir Guard wird automatisch gestartet.
 - Es wird keine Lizenzdatei kopiert, d. h. AntiVir arbeitet zunächst als Demoversion.
- Aktivieren Sie **Express setup** und klicken Sie auf **Next**.
- ↳ Ein Dialogfenster erscheint, in dem alle Einstellungen und weitere Anweisungen angezeigt werden.
- Klicken Sie auf **Install**.
- ↳ Das Programm wird installiert.

Custom setup

Sie können das Programm auch mit benutzerdefinierten Einstellungen installieren.

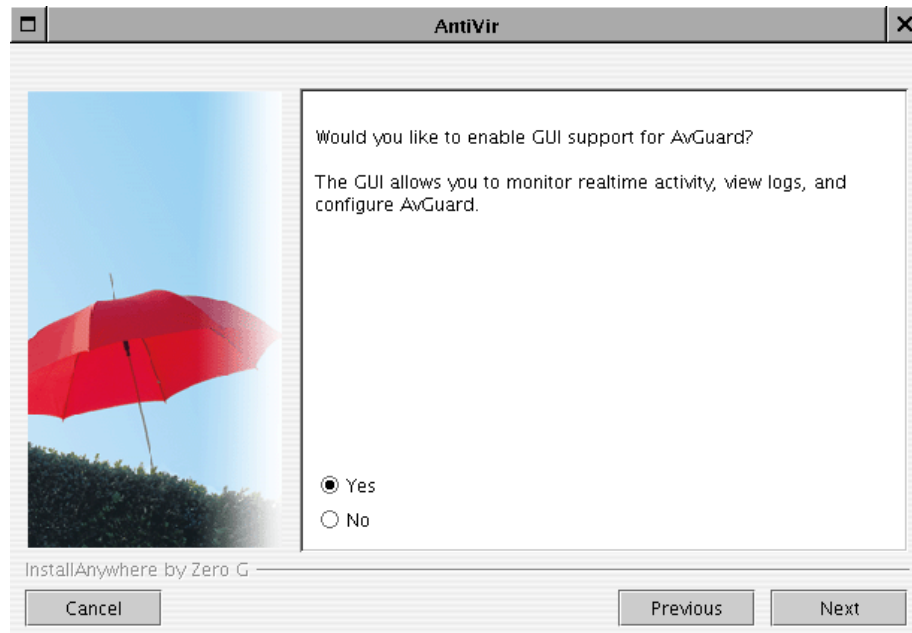
- Aktivieren Sie **Custom setup** und klicken Sie auf **Next**.
- ↳ Im folgenden Dialogfenster wird abgefragt, ob der AntiVir Guard installiert werden soll.



Sie haben drei Möglichkeiten, den AntiVir Guard zu installieren:

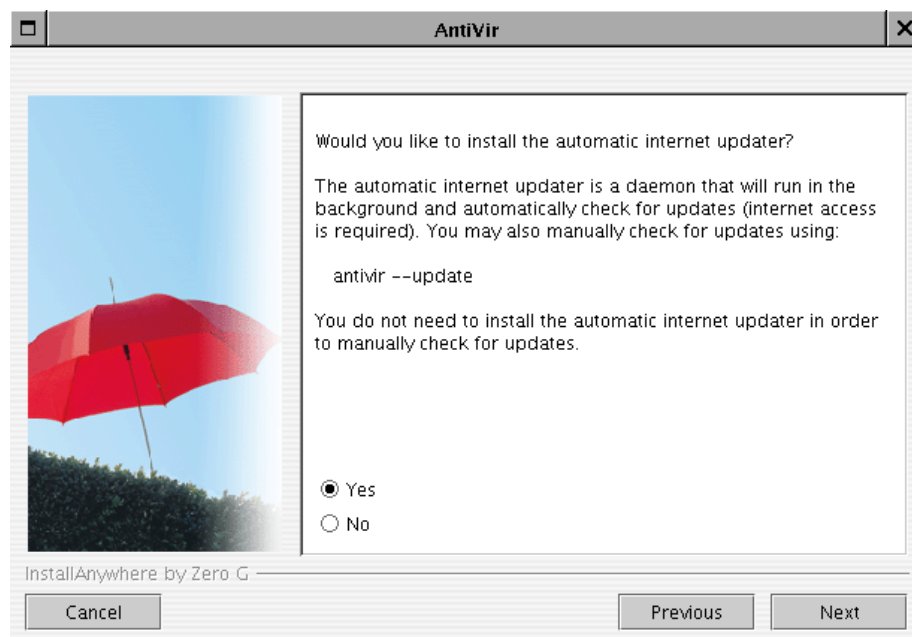
- **Auto install:** Die Quellen von Dazuko werden kompiliert und dem Kernel als Modul hinzugefügt.
 - **Manual install:** Das Kernel-Modul Dazuko wird manuell erstellt (siehe [Erstellen des Kernel-Moduls Dazuko](#) – Seite 12)
 - **No Install:** Der AntiVir Guard wird nicht installiert.
- Aktivieren Sie **Auto install**, um Dazuko automatisch zu installieren und klicken Sie auf **Next**.

- ↳ Im folgenden Dialogfenster wird abgefragt, ob die GUI-Unterstützung aktiviert werden soll (Eintrag in der Datei *avguard.conf*):



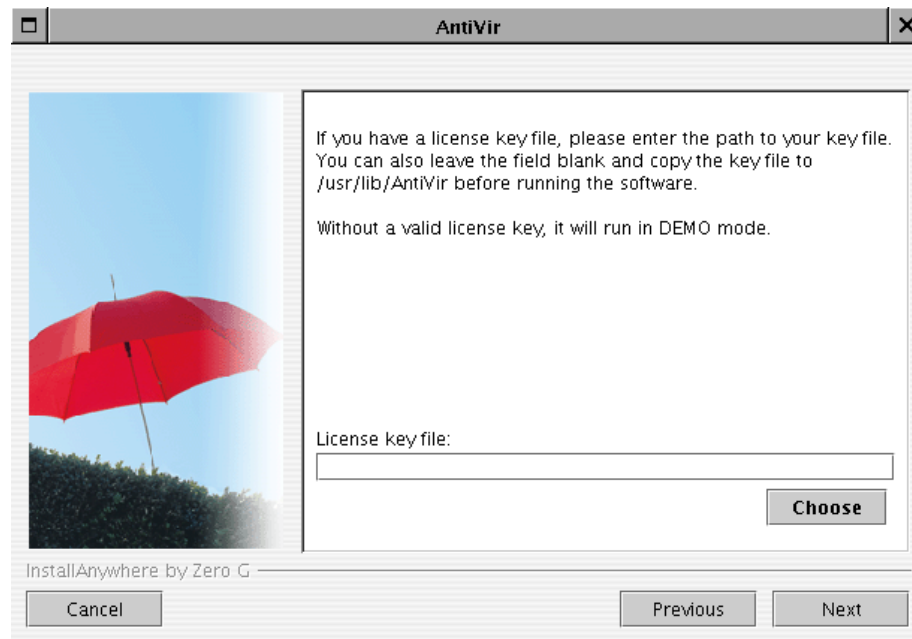
- ▶ Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.

- ↳ Im folgenden Dialogfenster wird abgefragt, ob der automatische Internet Update Daemon installiert werden soll:

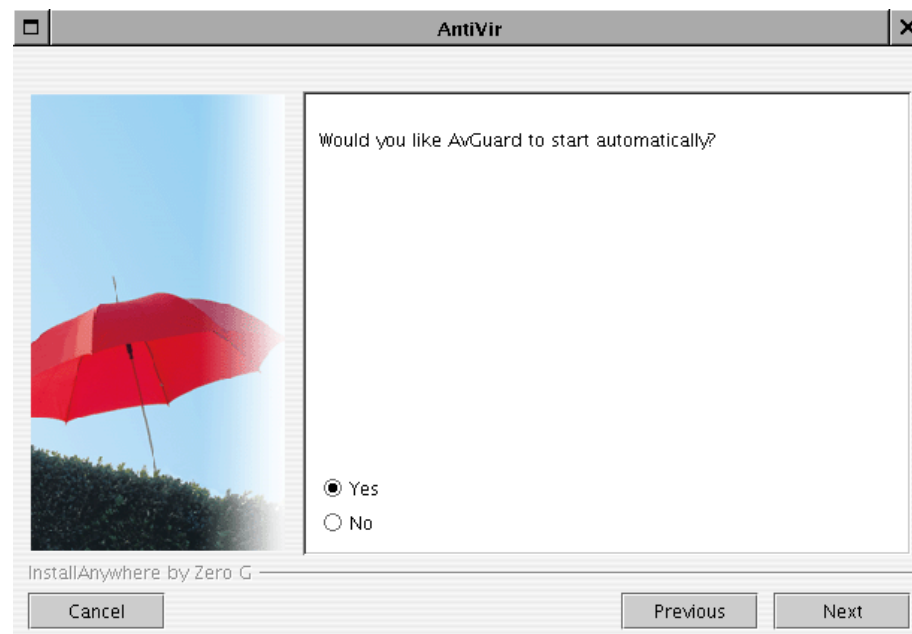


Wenn der Internet Update Daemon installiert werden soll:

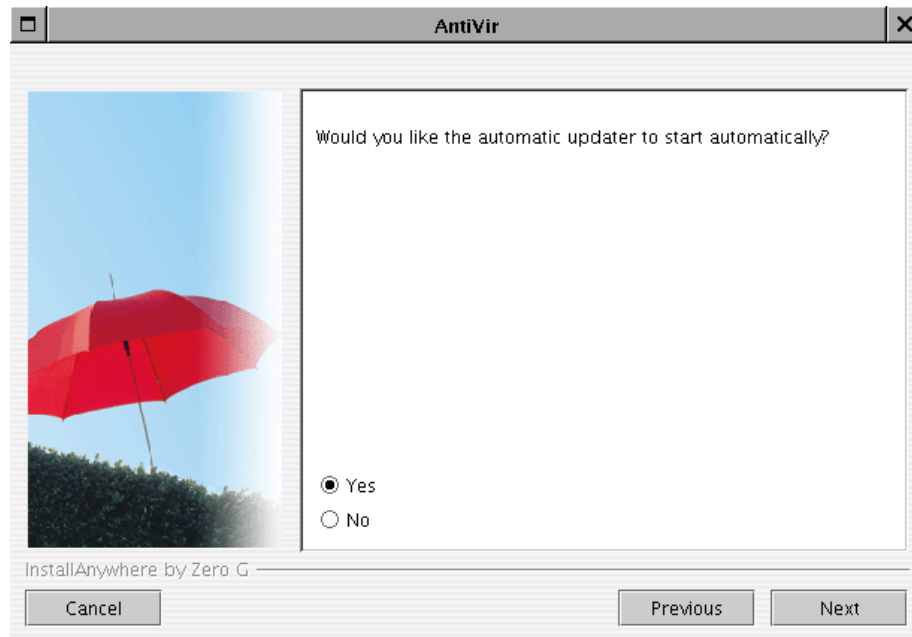
- ▶ Aktivieren Sie **Yes** und klicken Sie auf **Next** (in diesem Fall erscheint am Ende der Installation die Abfrage, ob der Update Daemon beim Booten des Rechners automatisch gestartet werden soll).
- ↳ Im folgenden Dialogfenster wird abgefragt, ob eine Lizenzdatei kopiert werden soll:



- Folgen Sie den Anweisungen und klicken Sie auf **Next**.
 - ↳ Im folgenden Dialogfenster wird abgefragt, ob der AntiVir Guard beim Booten des Rechners automatisch gestartet werden soll:

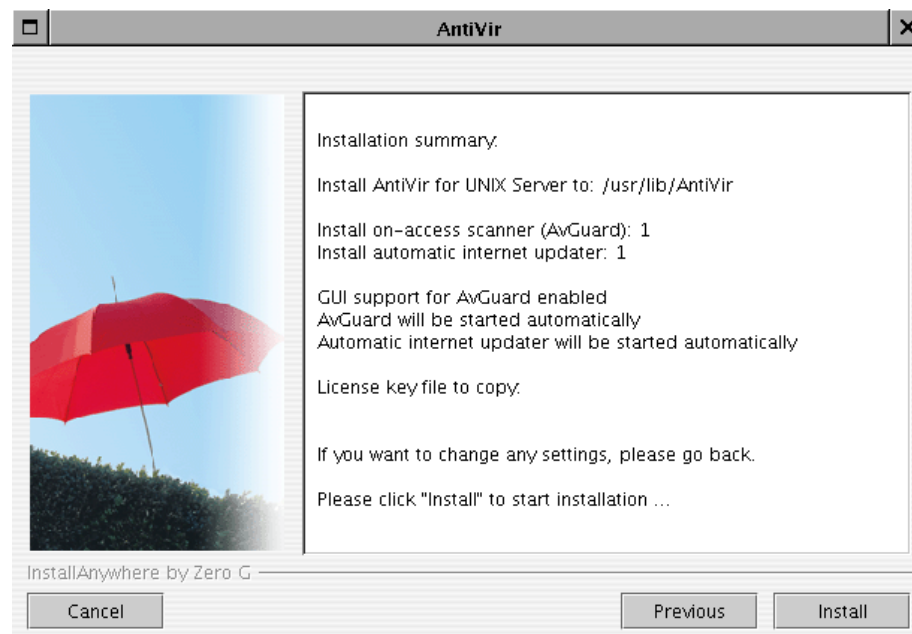


- Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.
 - ↳ Optional wird im folgenden Dialogfenster abgefragt, ob der Update Daemon beim Booten des Rechners automatisch gestartet werden soll:



- Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.

- ↳ Ein Dialogfenster erscheint, indem alle Einstellungen und weitere Anweisungen angezeigt werden:



- Klicken Sie auf **Install**.

- ↳ Das Programm wird installiert.

GUI only

Wählen Sie diese Installationsart, wenn Sie nur die GUI installieren wollen.

- Aktivieren Sie **GUI only** und klicken Sie auf **Next**.

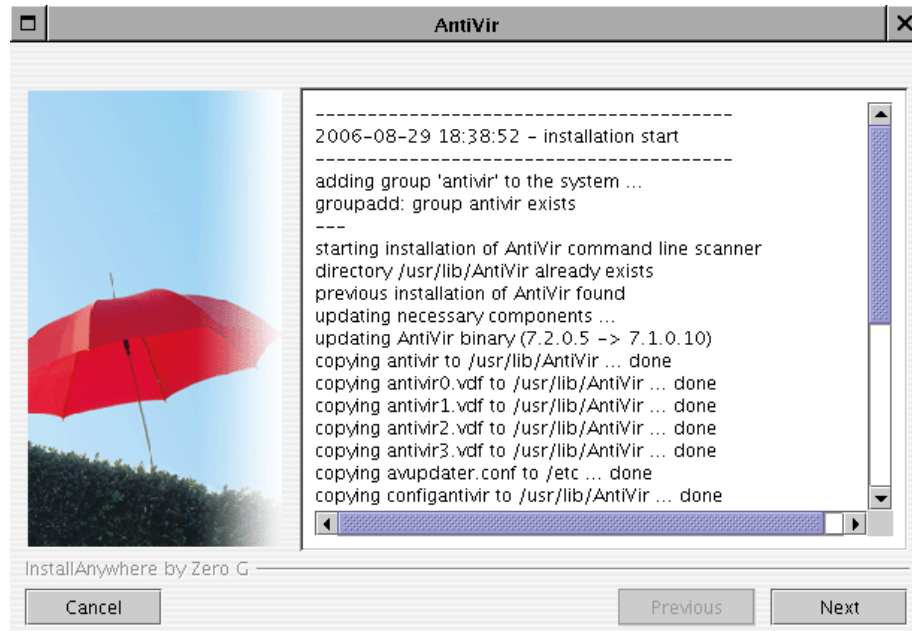
- ↳ Die GUI wird im folgenden Verzeichnis installiert:
`/usr/lib/AntiVir`

- ↳ Ein Dialogfenster erscheint, indem alle Einstellungen und weitere Anweisungen angezeigt werden:

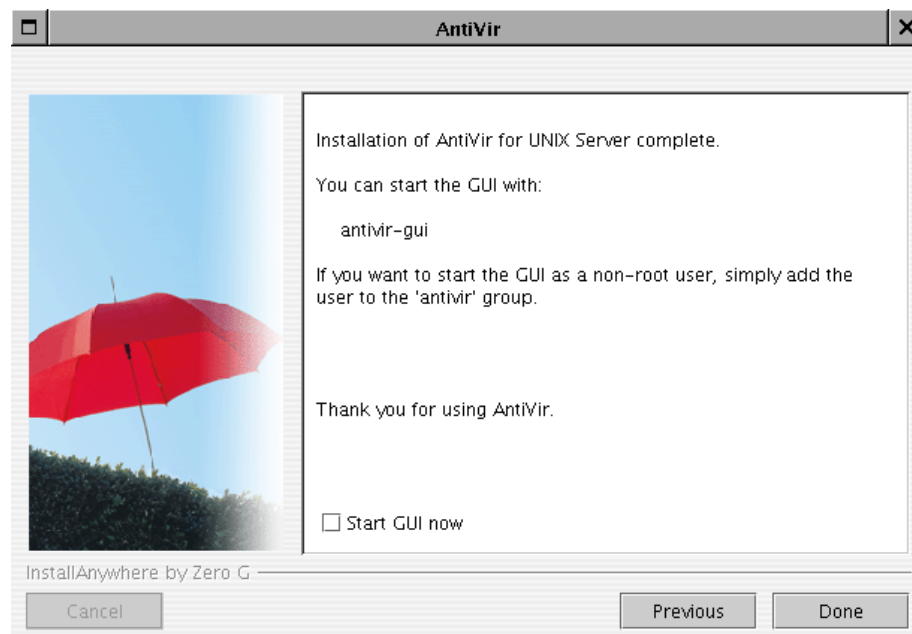
- Klicken Sie auf **Install**.
- ↳ Die GUI wird installiert.

Installation abschließen

Unabhängig davon, welche Installationsart Sie gewählt haben, erscheint ein Dialogfenster, in dem die einzelnen Installationsschritte aufgelistet sind:



- Klicken Sie auf **Next**.
- ↳ Das folgende Dialogfenster erscheint:



Wenn Sie die GUI starten wollen:

- Aktivieren Sie das Kontrollkästchen **Start GUI now**.
- Klicken Sie auf **Done**.

Die Installation ist abgeschlossen.

3.8 Anbindung an Produkte von Fremdherstellern

Einbindung in AMaViS

Das Projekt "A Mail Virus Scanner (AMaViS)" (<http://www.amavis.org/>) ist bereits für den Einsatz zusammen mit dem AntiVir-Scanner vorbereitet. AMaViS muss entweder nach der Installation von AntiVir installiert werden, so dass die automatische Erkennung stattfindet. Oder die Unterstützung von AntiVir muss beim Installieren von AMaViS explizit aktiviert werden, wahlweise mit den Optionen `--enable-all` oder `--enable-hbedv` für das Kommando `./configure`.



Bitte beachten Sie, dass AMaViS den Kommandozeilenscanner benutzt und diesen für jede einzelne Nachricht als separaten Prozess ausführt. Dieses Verfahren ist damit leider nicht so performant wie ein dedizierter Email-Scanner. Für Umgebungen mit höheren Anforderungen an den Durchsatz sollten Sie also den Einsatz von AntiVir MailGate oder von auf SAVAPI basierenden Produkten erwägen.



Für den Einsatz des Kommandozeilenscanners zusammen mit AMaViS ist eine Server-Lizenz erforderlich. Nur diese erlaubt es Antiviren-Scandienste für andere Rechner zu erbringen.

4 Konfiguration

Damit AntiVir UNIX Server optimal auf Ihrem System läuft, müssen Sie AntiVir konfigurieren. Bereits im Anschluß an die Installation haben Sie die Möglichkeit, die wichtigsten Einstellungen vorzunehmen. Dabei werden Ihnen Einstellungen vorgeschlagen, die für viele Fälle sinnvoll sind.

Sie können jederzeit nachträglich diese Einstellungen ändern und so AntiVir immer optimal anpassen.

Nach einer kurzen Übersicht werden Sie Schritt für Schritt in die Konfiguration eingeführt:

- Eine Übersicht über die Konfigurationsdateien erhalten Sie in [Konfigurationsdateien](#) – Seite 34.
- Erklärungen zum allgemeinen Umgang mit dem Konfigurationsscript erhalten Sie in [Konfigurationsscript](#) – Seite 42
- Spezifische Konfigurationen von AntiVir werden erläutert in
- [Konfigurieren des AntiVir Samba Scanners](#) – Seite 43
- [Konfigurieren regelmäßiger Updates](#) – Seite 46
- Abschließend wird in [AntiVir UNIX Server testen](#) – Seite 52 erklärt, wie Sie die korrekte Konfiguration von AntiVir prüfen.

4.1 Übersicht

Konfigurationsdateien

Die Konfiguration wird in drei Dateien definiert:

- *avguard.conf* definiert das Verhalten des residenten Wächters AntiVir Guard und die Protokollierung beim Auftreten von Viren und unerwünschten Programmen.
- *avupdater.conf* definiert das automatische Update der Software und die Protokollierung desselben.
- *vscan-antivir.conf* und *avsamba.conf* definieren das Verhalten des AntiVir Samba Scanners.



Die Einstellungen können direkt in den Konfigurationsdateien vorgenommen werden. Dies ist an sich nicht schwierig.

Komfortabler ist aber die Einstellung über Oberflächen wie Script oder GUI, die im Programmpaket enthalten sind. Diese Programme fangen eventuelle Fehleingaben ab und starten die notwendigen Prozesse neu.

Konfigurationsscript

In */usr/lib/AntiVir* steht das Script *configantivir* zur Verfügung. Dieses editiert die den Internet Updater beeinflussenden Einstellungen (also die Angaben in der Datei *avupdater.conf*).

4.2 Konfigurationsdateien

Dieser Abschnitt beschreibt den Aufbau der Konfigurationsdateien von AntiVir. Diese Dateien liest AntiVir beim Programmstart ein. Leerzeilen und Zeilen, die mit # beginnen, werden ignoriert.

Bei Lieferung sind Werte eingestellt, die für viele Anwendungen sinnvoll sind. Einige Einträge sind durch ein vorgestelltes # deaktiviert (auskommentiert) und können durch Entfernen des # aktiviert werden.



Wenn Sie manuell Werte in den Konfigurationsdateien ändern und nicht das Konfigurationsscript verwenden, müssen Sie anschließend den Internet Update Daemon und den AntiVir Guard manuell neu starten. Erst dann werden die Änderungen wirksam.

► Geben Sie dafür ein:

```
/usr/lib/AntiVir/avupdater restart  
/usr/lib/AntiVir/avguard restart
```

Konfigurationsdatei avguard.conf

Im Folgenden werden die Einträge in *avguard.conf* kurz beschrieben. Diese Einträge beeinflussen nur das Verhalten von AntiVir UNIX Server und nicht die anderen Programme von AntiVir. Wie Sie diese Einstellungen über eine grafische Benutzeroberfläche komfortabel editieren können, erfahren Sie in [AntiVir Guard über GUI konfigurieren](#) – Seite 78.

Num Daemons

Anzahl Dämonen:

Die Anzahl der AntiVir Guard-Dämonen, die gleichzeitig laufen, kann zwischen 3 und 20 eingestellt werden. Der voreingestellte Wert 3 ist sinnvoll für kleinere Standardrechner. Für leistungsfähige Industrie-PC kann eine höhere Anzahl sinnvoll sein:

NumDaemons 3

Wenn der Wert auf 0 gesetzt wird, wird der AntiVir Guard deaktiviert.

AccessMask

AccessMask:

In der Access Mask wird festgelegt, bei welchen Zugriffen der AntiVir Guard eine Datei auf Viren und unerwünschte Programme scannt:

- 1: Scannen bei Öffnen einer Datei
- 2: Scannen bei Schließen einer Datei
- 4: Scannen bei Ausführen einer Datei

Um einen Scan bei mehreren Zugriffsarten zu definieren, werden die obigen möglichen Werte für AccessMask addiert. Für Scannen bei Öffnen und Schließen einer Datei muss z. B. der Wert auf 3 gesetzt werden. Voreingestellt ist:

AccessMask 3



Bitte beachten Sie, dass AntiVir Guard nur auf diese Situationen reagieren und Dateien scannen kann, wenn das Kernel-Modul diese Ereignisse tatsächlich liefert. Nicht jedes Betriebssystem unterstützt alle Ereignisse in jeder Version des Kernels, zusätzlich können bei der Erzeugung des Kernel-Moduls einzelne Ereignisse an- oder abgewählt werden. Unabhängig von der Verwendung der anderen Ereignisse wird empfohlen, immer auch beim Öffnen von Dateien scannen zu lassen.

Repair Concerning Files **Reparatur von Dateien:**
Der AntiVir Guard ist in der Lage, Dateien sofort beim Zugriff zu reparieren. Schlägt dies fehl, wird der Zugriff geblockt. Hierfür muss folgende Option aktiviert werden:

```
RepairConcerningFiles yes
```

In der Voreinstellung ist diese Option deaktiviert.

LogOnly, Rename..., Move... **Aktion bei Funden von Viren oder unerwünschten Programmen:**
Wenn `RepairConcerningFiles` nicht eingestellt ist oder die Reparatur nicht möglich ist, wird der Zugriff auf die Datei gesperrt und der Vorgang protokolliert. Über folgende drei Optionen werden weitere Aktionen vom AntiVir Guard definiert:

- `LogOnly`: keine weiteren Aktionen
- `RenameConcerningFiles`: Umbenennen der Datei durch Anhängen der Endung `.XXX`
- `MoveConcerningFilesTo`: Verschieben der Datei in ein beliebiges auszuwählendes Verzeichnis. Dieses Verzeichnis wird automatisch angelegt, wenn es noch nicht existiert. Beispiel:

```
MoveConcerningFilesTo /home/unwanted
```

Nur eine der drei Optionen kann eingestellt sein, AntiVir wählt jeweils die letzte in der Konfigurationsdatei aufgeführte aus.

IncludePath **Überwachte Verzeichnisse:**

Der AntiVir Guard scannt die Dateien im angegebenen Verzeichnis inklusive aller Unterverzeichnisse.

Die Daten der verschiedenen Nutzer liegen üblicherweise unter `/home`. Entsprechend ist die Voreinstellung:

```
IncludePath /home
```

Pro Eintrag ist nur ein Verzeichnis zugelassen. Mehrere Verzeichnisse können angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile. Beispiel:

```
IncludePath /home
```

```
IncludePath /var
```



Wenn kein Verzeichnis angegeben wird, überwacht der AntiVir Guard keine Dateien!

ExcludePath **Ausgeschlossene Verzeichnisse:**

Der AntiVir Guard kann einzelne Verzeichnisse von der Überwachung ausnehmen, z. B. ein Verzeichnis, in das temporäre Dateien von AntiVir-Komponenten gelegt werden. Eine Voreinstellung gibt es nicht.

Pro Eintrag ist nur ein Verzeichnis zugelassen. Mehrere Verzeichnisse können natürlich trotzdem angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile. Beispiel:

```
ExcludePath /home/log
```

```
ExcludePath /home/tmp
```



Wenn Sie `MoveConcerningFilesTo` gewählt haben, wird dieses Verzeichnis automatisch auch als `ExcludePath` interpretiert.

ArchiveScan	<p>Überwachte Archive:</p> <p>Der AntiVir Guard scannt zusätzlich komprimierte Archive beim Zugriff, abhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio. Hierfür muss folgende Option aktiviert werden:</p> <p>ArchiveScan yes</p> <p>In der Voreinstellung ist diese Option deaktiviert, um die Performance von AntiVir möglichst hoch zu halten.</p>
ArchiveMax Size	<p>Maximale Archivgröße:</p> <p>Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die im unkomprimierten Zustand kleiner als ArchiveMaxSize (in Bytes) sind. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt ist 1 GByte (1073741824 Bytes):</p> <p>ArchiveMaxSize 1073741824</p>
ArchiveMax Recursion	<p>Rekursionstiefe für Archive:</p> <p>Wenn rekursiv gepackte Archive gescannt werden, kann die Rekursionstiefe auf ArchiveMaxRecursion beschränkt werden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:</p> <p>ArchiveMaxRecursion 20</p>
Archive MaxRatio	<p>Dekompressionsfaktor für Archive:</p> <p>Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die einen vorgegebenen Dekompressionsfaktor nicht überschreiten. Diese Maßnahme schützt vor so genannten "Mailbomben", die beim Dekomprimieren unerwartet viel Speicherplatz belegen würden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:</p> <p>ArchiveMaxRatio 150</p>
Archive MaxCount	<p>Anzahl Dateien innerhalb eines Archivs:</p> <p>Das Scannen von Archiven wird auf die vorgegebene Anzahl von Dateien innerhalb eines Rekursionsschrittes beschränkt. Bei einem Wert von 0 findet keine Beschränkung statt. Es ist kein Wert voreingestellt.</p> <p>ArchiveMaxCount 0</p>
Detect...	<p>Erkennung weiterer unerwünschter Programme:</p> <p>Neben Viren existieren noch andere Arten von Software, die Schaden anrichten können oder aus anderem Grund unerwünscht sind. Die Erkennung dieser Software kann mit folgenden Optionen aktiviert werden. Die Erkennung von Viren ist nicht optional und kann nicht deaktiviert werden.</p> <p>Die Voreinstellungen sind:</p> <p>DetectAdspy yes</p> <p>DetectBDC yes</p> <p>DetectDial yes</p> <p>DetectGame no</p> <p>DetectJoke no</p> <p>DetectPck no</p> <p>DetectPhish yes</p> <p>DetectSPR no</p>

Das Schlüsselwort "DetectAllTypes" kann verwendet werden, um mit einer einzigen Angabe alle bekannten Kategorien zu aktivieren.

Heuristics **Makroviren-Heuristik:**

Macro Aktiviert die Heuristik für Makroviren in Dokumenten. In der Voreinstellung ist diese Option aktiviert.

HeuristicsMacro yes

Heuristics **Win32-Datei-Heuristik:**

Level Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein. Zulässige Werte sind 0 (aus), 1 (niedrig), 2 (mittel) und 3 (hoch). Voreingestellt:

HeuristicsLevel 0

ScanMode **Konfiguration zu scannender Dateien:**

Mit diesem Eintrag wird festgelegt nach welchem Verfahren bestimmt wird ob eine Datei zu scannen ist. Mögliche Werte sind:

- extlist: nur Dateien scannen, deren Namen mit einer bestimmten Kennung enden;
- smart: Dateien aufgrund sowohl ihres Namens als auch unter Einbeziehung ihres Dateityps scannen;
- all: Dateien unbesehen ihres Typs oder Namens immer scannen.

Voreingestellt ist, dass alle Dateien überprüft werden:

ScanMode all



Um die folgende Programmfunktion nutzen zu können, wird der Einsatz von Dazuko 2.0.0 oder höher vorausgesetzt.

External
Program

Start eines externen Prozesses bei Fund verdächtiger Dateien:

Wird ein Virus bzw. unerwünschtes Programm gefunden, kann der AntiVir Guard einen externen Prozess starten. Dieser kann eine über die Fähigkeiten des AntiVir Guard hinausgehende Benachrichtigung veranlassen oder eine sonstige Nachbereitung übernehmen.

Möglich sind z. B. der Versand einer SMS, der Anruf eines Verantwortlichen, die Anzeige eines Dialogfensters am lokalen Bildschirm oder auch an einem entfernt stehenden Windows-Rechner, das Speichern der vorliegenden Daten in einem anderen Format oder in einer Datenbank.

Vor dem Start werden Platzhalter (mit % beginnende Sequenzen) durch die konkreten Daten des auslösenden Ereignisses ersetzt. Dies ermöglicht eine differenzierte Behandlung und die Anpassung an lokale Gegebenheiten.

Die folgende Aufstellung listet die unterstützten Platzhalter und ihre Ersetzung auf:

Option	Funktion
%h	Verzeichnis, in dem sich die Datei befindet, kann Sonderzeichen enthalten
%f	Dateiname ohne Verzeichnis-Anteil, kann Sonderzeichen enthalten
%p	Vollständiger Dateiname inklusive Verzeichnis (gleich wie %h/%f), kann Sonderzeichen enthalten

Option	Funktion
%U	UID der Datei (numerische Account-Bezeichnung des Eigentümers)
%G	GID der Datei (numerische Account-Bezeichnung der UNIX-Gruppe)
%s	Dateigröße
%m	Zugriffsrechte der Datei
%De	Typ des auslösenden Ereignisses
%DF	Dateisystem/Partition, auf dem/der sich die Datei befindet
%Dp	PID des zugreifenden Prozesses
%Du	UID, unter der der zugreifende Prozess läuft
%Df	Flags der ausgeführten Datei-Operation
%Dm	Zugriffsmodus der ausgeführten Datei-Operation
%Sn	Bezeichnung des gefundenen Virus bzw. der gefundenen unerwünschten Software
%Sa	Zusatz-Informationen (falls verfügbar)
%St	Typ des gefundenen Virus bzw der unerwünschten Software
%SA	vom AntiVir Guard ausgeführte Aktion
%Su	Benutzer, der die Dateioperation ausgeführt hat



Einige der übergebenen Parameter werden nicht von AntiVir geprüft, sondern aus den Datei-Eigenschaften übernommen und an den gestarteten Prozess weitergegeben. Sie sollten deshalb vor der weiteren Verarbeitung geprüft werden.

```
ExternalProgram /usr/bin/logger -- blocking access to %p (%Sn)
```

GUISupport Unterstützung durch grafische Benutzeroberfläche (GUI):
Dieser Eintrag muss aktiviert sein, damit AntiVir mit der GUI kommunizieren kann.
Folgende Parameter müssen eingetragen sein:

```
GuiSupport      yes
GuiCAFile       /usr/lib/AntiVir/gui/cert/cacert.pem
GuiCertFile     /usr/lib/AntiVir/gui/cert/server.pem
GuiCertPass     antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht die GUI nicht zur Verfügung.

Mögliche Fehler werden in der log-Datei protokolliert.

EmailTo **Email-Nachrichten:**

AntiVir Guard kann Emails verschicken, wenn ein Virus oder unerwünschtes Programm entdeckt wurde. Eine Voreinstellung gibt es nicht. Um Emails zu verschicken muss ein Adressat angegeben werden, z.B.:

```
EmailTo root@localhost
```

Suppress Notification Below	<p>Email-Benachrichtigungen nach Dringlichkeit filtern:</p> <p>Mit dieser Einstellung kann gesteuert werden, dass Benachrichtigungen an die mit <code>EmailTo</code> konfigurierte Adresse nicht verschickt werden, wenn sie eine geringere als die vorgegebene Dringlichkeitsstufe haben. Es werden nur Benachrichtigungen verschickt, die der angegebenen oder einer höheren Stufe zugeordnet sind. Mögliche Werte für die Dringlichkeit (in aufsteigender Folge) sind <code>Notice</code>, <code>Information</code>, <code>Warning</code>, <code>Error</code> und <code>Alert</code>. In der Voreinstellung werden keine Benachrichtigungen verworfen.</p> <p><code>SuppressNotificationBelow Scanner Notice</code></p>
LogFile	<p>Logdatei:</p> <p>Alle wichtigen Operationen von AntiVir werden über den <code>syslog</code>-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B:</p> <p><code>LogFile /var/log/avguard.log</code></p>
Syslog...	<p>Syslog-Einstellung:</p> <p>Für alle wichtigen Operationen gibt AntiVir Meldungen an den <code>syslog</code>-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:</p> <p><code>SyslogFacility user</code> <code>SyslogPriority notice</code></p> <p>Diese Werte gelten auch, wenn die Einträge deaktiviert sind.</p>

Konfigurationsdatei `avupdater.conf`

Im Folgenden werden die Einträge in `avupdater.conf` kurz beschrieben. Diese Einträge beeinflussen den Internet Updater der AntiVir Software.

Diese Datei kann anstatt der manuellen Anpassung auch komfortabel mit der GUI editiert werden, sofern diese mit installiert wurde.



Wenn Sie manuell Werte in `avupdater.conf` ändern, müssen Sie anschließend den Internet Update Daemon neu starten. Erst dann werden die Änderungen wirksam.

► Geben Sie dafür ein:

```
/usr/lib/AntiVir/avupdater restart
```

EmailTo	<p>Email-Nachrichten:</p> <p>Der AntiVir Internet Updater kann Emails verschicken, wenn ein Update ausgeführt wurde oder Probleme aufgetreten sind. Eine Voreinstellung gibt es nicht. Um Emails zu verschicken muss ein Adressat angegeben werden, z.B.:</p> <p><code>EmailTo root@localhost</code></p>
Suppress Notification Below	<p>Email-Benachrichtigungen nach Dringlichkeit filtern:</p> <p>Mit dieser Einstellung kann gesteuert werden, dass Benachrichtigungen an die mit <code>EmailTo</code> konfigurierte Adresse nicht verschickt werden, wenn sie eine geringere als die vorgegebene Dringlichkeitsstufe haben. Es werden nur Benachrichtigungen verschickt, die der angegebenen oder einer höheren Stufe zugeordnet sind. Mögliche Werte für die Dringlichkeit (in aufsteigender Folge) sind <code>Notice</code>, <code>Information</code>, <code>Warning</code>, <code>Error</code> und <code>Alert</code>. In der Voreinstellung werden keine Benachrichtigungen verworfen.</p> <p><code>SuppressNotificationBelow Updater Notice</code></p>

LogFile	<p>Logdatei:</p> <p>Alle wichtigen Operationen von AntiVir werden über den <i>syslog</i>-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B:</p> <pre>LogFile /var/log/avupdater.log</pre>
Syslog...	<p>Syslog-Einstellung:</p> <p>Für alle wichtigen Operationen gibt AntiVir Meldungen an den <i>syslog</i>-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:</p> <pre>SyslogFacility user</pre> <pre>SyslogPriority notice</pre> <p>Diese Werte gelten auch, wenn die Einträge deaktiviert sind.</p>
AutoUpdate...	<p>Update-Plan:</p> <p>Die AntiVir Software kann mit Hilfe des Internet Update Daemon regelmäßig online auf Updates geprüft und, wenn nötig, aktualisiert werden. In der Voreinstellung sind diese Optionen deaktiviert, es wird also kein automatisches Update durchgeführt.</p> <p>Bitte aktivieren Sie (nach gegebenenfalls notwendiger Konfiguration der HTTP-Proxy-Parameter) einen Update-Plan und starten Sie den Update Daemon oder richten Sie einen Job im cron-Daemon ein, um die AntiVir Software stets auf aktuellem Stand zu halten.</p> <p>Für Updates alle 2 Stunden muss folgende Option aktiviert werden:</p> <pre>AutoUpdateEvery2Hours</pre> <p>Für tägliche Updates muss folgende Option aktiviert werden:</p> <pre>AutoUpdateDaily</pre> <p>Wenn tägliche Updates eingestellt sind, kann in einem weiteren Eintrag die Uhrzeit für die Updates als HH:MM angegeben werden, z. B.:</p> <pre>AutoUpdateTime 04:23</pre>
HTTPProxy...	<p>Proxyserver:</p> <p>Wenn der Rechner über einen HTTP-Proxyserver mit dem Internet verbunden ist, muss dies spezifiziert werden, damit der automatische Internet Updater korrekt arbeitet. Als Voreinstellung sind die Einträge deaktiviert; es wird also eine direkte Verbindung ins Internet angenommen. Eingestellt werden müssen:</p> <ul style="list-style-type: none">• HTTP-Proxyserver• Port• Username und Passwort, wenn diese für den HTTP-Proxyserver erforderlich sind. <p>Beispiel:</p> <pre>HTTPProxyServer proxy.domain.com</pre> <pre>HTTPProxyPort 8080</pre> <pre>HTTPProxyUsername username</pre> <pre>HTTPProxyPassword password</pre>
Updater Keeps Backups	<p>Der Internet-Updater ersetzt installierte Dateien durch neuere Versionen, sobald diese verfügbar sind. Auch wenn die Dateien erst nach umfangreichen Tests ersetzt werden, können Sie dennoch Backups der vorherigen Versionen anlegen.</p>

Wird diese Option aktiviert, werden unterhalb des Verzeichnisses */usr/lib/AntiVir* weitere Verzeichnisse mit dem Namensschema *updater-backup-YYYYmmdd-HHMMSS* angelegt und die ersetzten Dateien dort archiviert.



Falls Sie die Backup-Funktion des Internet-Updaters aktivieren, sollten Sie regelmäßig diese Verzeichnisse prüfen und alte Versionen von Hand entfernen.

GnuPG...

GnuPG-Einstellung:

Die Authentizität der AntiVir-Updates kann durch GnuPG verifiziert werden. Nähere Informationen hierzu siehe Abschnitt [Authentizität der Updates durch GnuPG verifizieren](#) – Seite 51. Wenn GnuPG verwendet wird, muss der Pfad zur GnuPG-Binärdatei angegeben werden, z. B.:

```
GnuPGBinary /usr/local/bin/gpg
```

Zusätzliche GnuPG-Optionen können über `GnuPGOptions` spezifiziert werden, in Abhängigkeit von der speziellen GnuPG-Installation. Normalerweise ist dies aber nicht nötig. In der Voreinstellung sind beide Einträge aus Sicherheitsgründen deaktiviert.

UpdateAction

Art der Update-Aktion einstellen:

Mit dieser Einstellung kann für zusätzliche Software-Komponenten (*mailgate* oder *webgate*) gesteuert werden, ob diese Komponente gar nicht behandelt werden soll, nur auf die Verfügbarkeit von Updates geprüft oder eine verfügbare neuere Version auf die lokale Festplatte kopiert wird. Die Zusatzkomponenten werden nicht automatisch ersetzt, diese Aktion bleibt dem Administrator vorbehalten. Auf diese Weise ist immer ein lokaler Test der neuen Version dieser Netzwerk-Dienste vor ihrem Einsatz möglich. Für die Scan-Engine und die VDF-Datenbasis werden Updates immer eingespielt und können nicht deaktiviert werden. Die Schlüsselwörter für die vorgegebene Aktion sind *none*, *check* oder *fetch*. Voreingestellt ist, dass nur für den Scanner Updates ausgeführt werden und für keine Zusatzkomponente eine Überprüfung auf neue Versionen ausgeführt wird:

```
UpdateAction mailgate none
```

```
UpdateAction webgate none
```

UpdateStoreDir

Speicherort für verfügbare Komponenten-Updates:

Sollte für eine zusätzliche Software-Komponente ein Update verfügbar sein und wurde mit der `UpdateAction` Option eingestellt, dass die neue Version auf den lokalen Massenspeicher zu holen ist (Aktion *fetch*), wird die entsprechende Datei in das mit `UpdateStoreDir` angegebene Verzeichnis abgelegt. Voreingestellt ist ein Verzeichnis unterhalb des Installationsverzeichnisses:

```
UpdateStoreDir /usr/lib/AntiVir/updcomp
```

Konfigurationsdatei *avsamba.conf*

Wird auf einem Dateiserver nicht der on access Scanner AntiVir Guard eingesetzt sondern der AntiVir Samba Scanner, so kann dieser in der Datei *avsamba.conf* Datei konfiguriert werden. Die in dieser Datei vorgenommenen Einstellungen wirken für alle per *samba-vscan* an den Samba-Service angebotenen Scanner-Prozesse.

Gegebenenfalls in der Datei *vscan-antivir.conf* eingetragene (AntiVir spezifische) Einstellungen übersteuern die Angaben aus der Datei *avsamba.conf*. Es wird aber empfohlen, in der Datei *vscan-antivir.conf* nur Samba bzw *samba-vscan* spezifische Einstellungen vorzunehmen und die AntiVir spezifischen Einstellungen in der Datei *avsamba.conf* zu hinterlegen.

In der Datei *avsamba.conf* können die folgenden Schlüsselworte verwendet werden, deren Bedeutung Sie bitte aus der Beschreibung der Datei *avguard.conf* entnehmen: EmailTo, Suppress..., LogFile, Syslog..., Detect..., Heur..., Archive..., Repair..., LogOnly/Rename.../Move..., ScanMode.

4.3 Konfigurationsscript

Mit Hilfe des Konfigurationsscripts kann der AntiVir Internet Updater komfortabel angepaßt werden. Dieses Script fängt eventuelle Fehleingaben ab und startet die notwendigen Prozesse neu.

Der Umgang mit dem Script ist sehr einfach. Wenn Sie den Internet Updater konfigurieren wollen:

- Geben Sie ein:
`/usr/lib/AntiVir/configantivir`

Das Script liest die aktuell in *avupdater.conf* gesetzten Werte ein und fragt systematisch ab, ob neue Werte gesetzt werden sollen. Die möglichen neuen Werte werden angezeigt, die bisherigen Angaben werden dabei als Standardwert vorgeschlagen.

Wenn Sie einen vorhandenen Wert übernehmen wollen:

- Drücken Sie Enter.

Wenn Sie einen Wert ändern wollen:

- Geben Sie den neuen Wert ein.

Nach der Abfrage der einzelnen Werte wird eine Zusammenfassung der Konfiguration angezeigt und eine Bestätigung abgefragt:

```
AntiVir Configuration
=====
Here are the configuration settings you have specified. Look them over
to make sure they are correct.

email notification:      no
specific logfile:        /var/log/avupdater.log
update frequency:        every 2 hours (if update daemon is running)
http proxy server:       none

available options: y n
Save configuration settings? [y]
```

Wenn nicht alle Werte der gewünschten Konfiguration entsprechen:

- Geben Sie N ein, um das Konfigurationsscript neu zu starten und die falschen Werte zu korrigieren.

Wenn alle Angaben der gewünschten Konfiguration entsprechen:

- Bestätigen Sie mit Y oder Enter, um die Konfigurationsdatei mit den neuen Werten abzuspeichern.

- ↳ Das Script meldet die Speicherung der Konfigurationsdatei. Es gibt Informationen zum Umgang mit dem Internet Updater aus:

```
* SUCCESS *
Configuration successfully saved to.
/etc/avupdater.conf

Press <ENTER> to continue.

Running Internet Update Daemon
=====
In order for the Internet Update Daemon to be active
...
available options: y n
Would you like to apply the new configuration? [y]
```

- Geben Sie Y oder Enter ein, um den AntiVir Update Daemon zu starten.
 - ↳ Der Internet Update Daemon wird gestartet. Wenn der Daemon bereits läuft, wird er automatisch neu gestartet, damit die neuen Einstellungen wirksam werden. Damit ist die Konfiguration abgeschlossen:

```
Starting AntiVir: avupdater
...
AntiVir Status: avupdater running      [ running ]
Here are some commands that you should remember...

configure updater: /usr/lib/AntiVir/configantivir
start update daemon: /usr/lib/AntiVir/avupdater start
stop update daemon: /usr/lib/AntiVir/avupdater stop
update daemon status: /usr/lib/AntiVir/avupdater status
```

4.4 Konfigurieren des AntiVir Samba Scanners

Der AntiVir Samba Scanner besteht aus einem VFS Plugin für Samba und einem Scan Service. Für den Betrieb des AntiVir Samba Scanners muss das VFS Plugin (ein AntiVir-spezifisches Plugin für die samba-vscan-Software), wie im Kapitel [Anbindung an Samba](#) – Seite 14 beschrieben, installiert werden.

In der Konfigurationsdatei *smb.conf* des Samba Service muss für die zu überwachenden Freigaben (shares) das AntiVir VFS Plugin aktiviert werden. Die Angabe einer Konfigurationsdatei ist optional. Die neu hinzuzufügenden Einträge sehen z. B. so aus:

```
[myshare]
...
vfs object = vscan-antivir
vscan-antivir: config-file =
/usr/local/samba/lib/vscan-antivir.conf
```

Eventuell hat Ihr Distributor diesen Schritt bereits getan oder bietet eine Möglichkeit, ihn mit Hilfe einer Konfigurations-Oberfläche durchzuführen.

Sie können den Scanner für einzelne Shares oder – wenn Sie den entsprechenden Eintrag in der *[global]*-Section der Datei *smb.conf* vornehmen – für den ganzen Server aktivieren.

Sie können einzelne Shares mit separaten Konfigurationsdateien betreiben oder auch eine Konfigurationsdatei für alle Scanner gemeinsam verwenden. Wird keine Konfigurationsdatei für den Scanner angegeben, wird dieser in der Standardkonfiguration betrieben.

Konfigurationsdatei *vscan-antivir.conf*

Im Folgenden werden die Einträge in *vscan-antivir.conf* in der Reihenfolge ihres Auftretens kurz beschrieben. Die Einträge lassen sich grob in zwei Kategorien einteilen:

- in die samba-vscan-Optionen, die von allen Backends gleichermaßen unterstützt werden,
- in die AntiVir-spezifischen Optionen, die besondere Funktionen dieses Backends steuern.

Es wird empfohlen, in der Datei *vscan-antivir.conf* nur die samba-vscan spezifischen Einstellungen vorzunehmen und die AntiVir spezifischen Einstellungen in der Datei *avsamba.conf* abzulegen. Nicht alle für den AntiVir Samba Scanner relevanten Einstellungen können in der Datei *vscan-antivir.conf* stattfinden weil möglicherweise die betreffenden Schlüsselwörter (noch) nicht bekannt sind.

max file size

Maximale Dateigröße:

samba-vscan kann Dateien vom Scan ausschließen, die eine bestimmte Größe überschreiten. Wird dieser Wert auf 0 (Voreinstellung) gesetzt, werden alle Dateien untersucht.

```
max file size = 0
```

verbose file
logging

Einträge über Dateizugriffe im Log:

samba-vscan kann jeden Dateizugriff im Log vermerken (wenn dieser Wert auf `yes` gestellt wird) oder nur die Zugriffe auf Dateien, in denen ein Virus bzw. unerwünschtes Programm entdeckt wurde (`no`). Die Voreinstellung ist `no`.

```
verbose file logging = no
```

scan on open/
scan on close

Dateien beim Öffnen und/oder Schließen untersuchen:

samba-vscan kann Dateien beim Öffnen und/oder Schließen auf verschiedene Ereignisse hin untersuchen (Voreinstellung: in beiden Fällen).

```
scan on open = yes
```

```
scan on close = yes
```

deny access on
error/
deny access on
minor error

Zugriff auf Dateien verweigern:

samba-vscan kann den Zugriff nicht nur verweigern, wenn ein Virus bzw. unerwünschtes Programm in der Datei gefunden wurden, sondern auch, wenn bei der Verarbeitung der Datei ein Fehler auftritt. Diese Einstellung kann für verschiedene Fehler-Stufen vorgenommen werden:

Ist der Scanner selbst nicht verfügbar, gilt das als Fehler.

Ist der Scanner zwar erreichbar, konnte aber die Datei nicht scannen, gilt das als ein milderer Fehler.

Weil in diesen Situationen Schadsoftware unerkannt ins System gelangen kann, wird standardmäßig auch in diesen Fällen der Zugriff verweigert.

```
deny access on error = yes
```

```
deny access on minor error = yes
```

send warning message
Nachricht bei verweigertem Zugriff auf Datei:
 samba-vscan kann bei verweigertem Zugriff auf eine Datei den entfernten Nutzer des Dateiservers per Popup benachrichtigen (Voreinstellung: yes).
`send warning message = yes`

concerning file action (infected file action)
Datei-Aktionen:
 samba-vscan kann nicht nur den Zugriff auf betroffene Dateien verweigern, sondern auch zusätzliche Aktionen auslösen:

- Löschen der Datei
- Verschieben der Datei in einen Quarantäne-Bereich

Die entsprechenden Werte für diese Option sind `nothing` (Voreinstellung), `delete` und `quarantine`.



Beachten Sie, dass bei Erkennen von anderer unerwünschter Software als Viren die Bezeichnung "infected" nicht korrekt ist. Nicht alle Fundstellen sind mit einem Virus infiziert, sondern können einen anderen Anlaß haben. Aus diesem Grund wird aus Gründen der Kompatibilität zwar noch die Option `infected file action` erkannt, aber für neue Installationen die Verwendung von `concerning file action` empfohlen. Beachten Sie diesen Umstand auch, wenn Sie den Benachrichtigungstext für den betroffenen Nutzer erstellen.

`concerning file action = quarantine`

quarantine directory, quarantine prefix
Quarantäneverzeichnis und -präfix:
 Ist als Reaktion auf einen Virus oder ein unerwünschtes Programm das Verschieben in die Quarantäne aktiviert, kann mit diesen Parametern beeinflusst werden, in welchem Verzeichnis die Quarantäne liegt und mit welchem Präfix die Dateinamen versehen werden sollen. Passen Sie diese Einstellungen an die Gegebenheiten auf Ihrem System an. Schlägt das Verschieben betroffener Dateien in das angegebene Verzeichnis fehl, werden sie vom Massenspeicher gelöscht.

`quarantine directory = /tmp`
`quarantine prefix = vir-`

max lru files entries, lru file entry lifetime
Zuletzt untersuchte Dateien:
 samba-vscan erstellt eine Liste der zuletzt untersuchten Dateien, um bei kurz aufeinander folgenden Zugriffen schneller reagieren zu können und unnötige Scan-Vorgänge einzusparen. Mit diesen Einstellungen läßt sich der Speicher der zuletzt benutzten Dateien (LRU=last recently used) konfigurieren. Voreinstellung: 100 Einträge für bis zu fünf Sekunden.

`max lru files entries = 100`
`lru file entry lifetime = 5`

exclude file types
Dateien vom Scan ausschließen:
 samba-vscan kann Dateien eines bestimmten Typs vom Scan ausschließen, wobei diese Klassifizierung nach dem MIME-Typ der Datei geschieht. Diese Einstellung sollte mit sehr viel Vorsicht eingesetzt werden!

Voreingestellt ist eine leere Liste, d. h. es werden keine Dateien vom Scan ausgenommen.
`exclude file types =`

antivir program **Pfad für antivir-Programm:**
name Das VFS Plugin dient als Schnittstelle zwischen Samba und dem Scan Service. Für den AV Scan wird das "antivir"-Programm eingesetzt. Mit dieser Einstellung wird dem Plugin mitgeteilt, an welcher Stelle sich das "antivir"-Programm befindet. Voreinstellung:
`/usr/lib/AntiVir/antivir.`

```
antivir program name = /usr/lib/AntiVir/antivir
```

Optionen für **Archive prüfen:**
Archive Der AntiVir Samba Scanner kann auch innerhalb von Archiven nach betroffenen Dateien suchen, wenn die Option `antivir scan in archive` auf `yes` eingestellt wird. Dabei werden Dateien nicht vollständig untersucht, wenn sie eines der eingestellten Limits (maximales Kompressionsverhältnis, maximale Größe des Inhalts, maximale Schachtelungstiefe weiterer Archive im Inhalt) überschreiten. Ein Wert von 0 für eines dieser Limits setzt es außer Kraft bzw auf "unendlich".

```
antivir scan in archive = no
```

```
antivir max ratio in archive = 150
```

```
antivir max archived file size = 1073741824
```

```
antivir max recursion level = 5
```

antivir detect ... **Suche nach unerwünschter Software:**
Der AntiVir Samba Scanner sucht in übergebenen Dateien immer nach Viren. Zusätzlich können auch andere Arten von unerwünschter Software erkannt werden, wenn die entsprechende Option aktiviert (auf `yes` gesetzt) wird.



Bitte beachten Sie den bei der Option `concerning file action` bereits erwähnten Sachverhalt, dass die Verweigerung des Zugriffs in diesem Fall nicht notwendigerweise bedeuten muss, dass die betroffene Datei mit einem Virus infiziert ist. Als Voreinstellung wird ausschließlich nach Viren gesucht.

```
antivir detect dialer = no
```

```
antivir detect game = no
```

```
antivir detect joke = no
```

```
antivir detect pms = no
```

```
antivir detect spy = no
```

Als Kurzform für die Aktivierung aller `detect`-Optionen gibt es die Option `antivir detect alltypes`. Wird diese Option auf `yes` gesetzt, wirkt das als wären alle oben aufgeführten Optionen mit dem Wert `yes` einzeln aufgeführt worden.

4.5 Konfigurieren regelmäßiger Updates

Die Leistungsfähigkeit und Wirksamkeit einer Virensoftware steht und fällt mit ihrer Aktualität. Deshalb bietet AntiVir die Möglichkeit, jederzeit Updates über HTTP vom AntiVir-Webserver zu laden, und dies auf Wunsch auch automatisiert in regelmäßigen Abständen.

Bei diesen Updates werden die Bestandteile von AntiVir, die den Schutz vor Viren und unerwünschten Programmen sicherstellen, auf den neuesten Stand gebracht.

Alle Update-Prozesse verwenden den AntiVir Kommandozeilenscanner.

Der Befehl `antivir --update` ermöglicht zu jeder Zeit eine Aktualisierung der AntiVir-Software, siehe [AntiVir manuell aktualisieren](#) – Seite 60.

Sie haben zwei unterschiedliche Möglichkeiten, automatische Updates von AntiVir zu konfigurieren:

- Sie verwenden den mitgelieferten Internet Update Daemon, den Sie einfach konfigurieren können. Dies ist empfohlen, wenn Sie geringe UNIX-Kenntnisse haben und wenig eigene Anpassungen vornehmen möchten.
- Sie verwenden AntiVir in Verbindung mit dem cron-Dämon. Dies ist empfohlen, wenn Sie vertiefte UNIX-Kenntnisse haben. Hier müssen Sie die Konfiguration selbst vornehmen, haben dadurch aber mehr Spielraum.

Internet-Zugang für Updates konfigurieren

- ✓ Stellen Sie sicher, dass Ihr Internetzugang funktioniert. In den meisten Fällen wird der Internetzugang bereits konfiguriert sein. Ansonsten entnehmen Sie die notwendigen Informationen Ihrer UNIX-Dokumentation.

Proxyserver Falls Sie über einen HTTP-Proxyserver mit dem Internet verbunden sind, müssen Sie AntiVir entsprechend konfigurieren:

- ▶ Rufen Sie `configantivir` auf:
`/usr/lib/AntiVir/configantivir`
- ▶ Bestätigen Sie die Einstellungen mit Enter, bis die Abfrage zum Proxyserver kommt:

HTTPProxyServer/HTTPProxyPort (4 of 4)

=====

If this machine is sitting behind an HTTP proxy server, you will need to configure AntiVir with the appropriate proxy settings. Internet access is required in order to make updates.

available options: y n

Does this machine use an HTTP proxy server? [n]

- ▶ Geben Sie Y ein.
 - ↳ Anschließend wird nach dem Namen und dem Port des Proxyservers gefragt. Geben Sie die Daten ein:

What is the HTTP proxy server name? [] proxy.domain.tld

Which port number does the HTTP proxy server use? [] 3128

- ↳ Anschließend wird gefragt, ob für den Proxyserver ein Username und ein Passwort notwendig sind:

HTTPProxyUsername/HTTPProxyPassword (4-2 of 4)

=====

Proxy servers may be configured to require a username and password. If the HTTP proxy server for this machine requires a username and password AntiVir needs to be appropriately configured.

available options: y n

Does the HTTP proxy server require a username/password? [n]

Wenn ein Username und Passwort erforderlich sind:

- ▶ Geben Sie Y ein.
 - ↳ Anschließend werden Sie nach Username und Passwort gefragt.

- Geben Sie Username und Passwort ein.

Das Konfigurationsskript zeigt die Zusammenfassung der Einstellungen an und fragt nach der Bestätigung um die Konfigurationsdatei zu schreiben.

Der Internet-Zugang für Updates ist konfiguriert.

Automatische Updates über den Internet Update Daemon konfigurieren

Der Internet Update Daemon ist ein sehr einfacher Dienst, der in festgesetzten Abständen folgenden Befehl aufruft:

```
antivir --update
```



Damit die nachfolgenden Einstellungen wirksam werden können, muss der Internet Update Daemon installiert sein. Wenn Sie die Installation wie unter [AntiVir installieren](#) – Seite 16 beschrieben vorgenommen haben, ist dies auch der Fall. Ansonsten müssen Sie nochmals das Installationsskript laufen lassen, siehe [AntiVir erneut installieren](#) – Seite 23.

Folgende Einstellungen können definiert werden:

- Abstände der Aktualisierung. Möglich ist
 - Update alle zwei Stunden
 - Tägliches Update
 - Zeitpunkt der Aktualisierung (bei täglichem Update). Möglich ist
 - Vom Benutzer eingestellter Zeitpunkt
 - Zufällig gewählter Zeitpunkt. Das Skript wählt in diesem Fall einmalig eine zufällige Zeit, die dann aber fest gesetzt wird. Dies ist dann sinnvoll, wenn der Rechner permanent online ist.
- Rufen Sie *configantivir* auf:
`/usr/lib/AntiVir/configantivir`

- Bestätigen Sie die Einstellungen mit **Enter** bis die Frage nach der Häufigkeit der Updates erscheint:

```
AutoUpdateEvery2Hours/AutoUpdateDaily          (3 of 4)
=====
AntiVir is equipped with an Internet Update Daemon. At specified
intervals, AntiVir will connect to an update server to check for newer
versions of the AntiVir engine or the data files. If a newer
version is available, AntiVir will automatically download and install
the updates without requiring any special attention. This allows AntiVir
to be kept current against attacks and problems.

AntiVir can be configured to check for updates every 2 hours (2) or
once a day (d). You can also choose to disable the Internet Update
Daemon (n).

Note: Updates can also be done manually from the command line:
    antivir --update
You may prefer to disable the Internet Update Daemon and
instead perform regular updates using a cron(8) job.

Using the startup script for the Internet Update Daemon when
it is disabled will result in an error.

available options: 2 d n
How often should AntiVir check for updates? [2]
```

- Wählen Sie
- n, wenn Sie keine automatischen Updates durchführen wollen
 - 2 für Updates alle zwei Stunden
 - d für tägliche Updates
- ↳ Wenn Sie tägliche Updates gewählt haben, wird nach dem Zeitpunkt des Updates gefragt:

```
AutoUpdateTime                                  (3-2 of 4)
=====
The AntiVir Updater can be set to always check for updates at a
particular time of day. This is specified in a HH:MM format
(where HH is the hour and MM is the minutes). If you do not have a
permanent connection, you may set it to a time when you are usually
online. You may also let AntiVir choose a random time (r).

If you have a permanent connection then a random time may be preferred
because it will help to disperse the times when other users are
getting updates.

available options: HH:MM r
What time should updates be done? [RANDOM]
```

- Geben Sie die Zeit im Format HH : MM ein
- ODER –
 - Geben Sie R für einen zufälligen Zeitpunkt ein.
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit Enter.

Die automatischen Updates über den Internet Update Daemon sind konfiguriert. Der Internet Update Daemon wird automatisch gestartet (wenn er noch nicht gelaufen war) beziehungsweise neu gestartet (wenn er bereits lief).

Internet Update Daemon manuell starten und anhalten

Wenn Sie den Internet Update Daemon starten wollen:

- ▶ Geben Sie ein:
`/usr/lib/AntiVir/avupdater start`

Wenn Sie den Internet Update Daemon anhalten wollen:

- ▶ Geben Sie ein:
`/usr/lib/AntiVir/avupdater stop`

Wenn Sie den aktuellen Status des Internet Update Daemon feststellen wollen:

- ▶ Geben Sie ein:
`/usr/lib/AntiVir/avupdater status`

Updates über Cron steuern



Die Steuerung mit dem Cron-Dämon wird empfohlen!

Wenn Sie vertiefte UNIX-Kenntnisse haben, können Sie den Cron-Dämon zur Steuerung der automatischen AntiVir-Updates nutzen.

Der Cron-Dämon steuert regelmäßig wiederkehrende Systemprozesse. Nähere Informationen hierüber entnehmen Sie Ihrer UNIX-Dokumentation.

Bei der Steuerung der Updates über den Cron-Dämon haben Sie mehr Konfigurationsmöglichkeiten als mit dem Internet Update Daemon.

- Beispiel ▶ Fügen Sie folgenden Cron-Job in `/etc/crontab` ein
- ```
45 */2 * * * root /usr/lib/AntiVir/antivir --update -q
```
- ↳ Dieser Eintrag bewirkt Updates alle zwei Stunden jeweils 15 Minuten vor der vollen Stunde, also um 0:45 Uhr, 2:45 Uhr, 4:45 Uhr und so weiter. Die Option `-q` bewirkt, dass keine Meldungen ausgegeben werden, siehe [Optionen](#) – Seite 53

### Internet Update Daemon automatisch starten

Wenn Sie nicht mit dem Cron-Dämon arbeiten wollen, benutzen Sie den Internet Update Daemon. Wenn Sie die Installation so vorgenommen haben, wie in [AntiVir installieren](#) – Seite 16 beschrieben, ist Ihr System schon entsprechend eingestellt.

Wenn der Internet Update Daemon noch nicht automatisch beim Systemstart gestartet wurde:

- ▶ Führen Sie die Installation (siehe [AntiVir erneut installieren](#) – Seite 23) mit den entsprechenden Einstellungen durch.

## Authentizität der Updates durch GnuPG verifizieren

GnuPG ist eine kostenlose Alternative zum Verschlüsselungsprogramm PGP (Pretty Good Privacy). Mit GnuPG kann die Authentizität der Updates von AntiVir verifiziert werden.

Die Verwendung von GnuPG wird sehr empfohlen.



Allerdings setzt die Verwendung vertiefte Kenntnisse von UNIX und GnuPG voraus. Bei fehlerhafter Konfiguration besteht ansonsten die Gefahr, dass AntiVir nicht mehr aktualisiert wird.

Diese Schritte müssen von dem Benutzer ausgeführt werden, der die Updates auf dem Rechner durchführt. Dies ist in den meisten Fällen der Benutzer mit Administratorrechten.

Weitere Informationen zu GnuPG enthalten Sie über <http://www.gnupg.org>

Führen Sie folgende Schritte durch, um die Unterstützung von GnuPG zu aktivieren:

- ▶ Laden Sie GnuPG von der GnuPG-Webseite <http://www.gnupg.org>. Hier erhalten Sie auch ein Handbuch mit weiterführenden Informationen zu PGP und dessen Anwendungsmöglichkeiten.
- ▶ Erzeugen Sie Ihren eigenen PGP-Schlüssel, wie in der GnuPG-Dokumentation beschrieben.
- ▶ Fügen Sie den öffentlichen AntiVir-PGP-Schlüssel zu Ihrem Schlüsselbund hinzu:  

```
gpg --import antivir.gpg
```

 – ODER –  
 Importieren Sie den öffentlichen AntiVir-PGP-Schlüssel direkt vom Keyserver:  

```
gpg --keyserver=wwwkeys.pgp.net --recv-keys 0F821C2E
```
- ▶ Fordern Sie den Fingerabdruck des Schlüssels an, um sicherzustellen, dass es tatsächlich der öffentliche AntiVir-PGP-Schlüssel ist:  

```
gpg --fingerprint build@avira.com
```

 ↳ Der 40-stellige Fingerabdruck wird ausgegeben.
- ▶ Stellen Sie sicher, dass der ausgegebene Fingerabdruck mit dem Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels übereinstimmt. Der Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels wird auf der Avira-Webseite (<http://www.avira.de>) angezeigt.
- ▶ Unterschreiben Sie den öffentlichen AntiVir-PGP-Schlüssel, um seine Gültigkeit zu beglaubigen:  

```
gpg --sign-key build@avira.com
```
- ▶ Wechseln Sie in das Unterverzeichnis */bin* Ihres AntiVir-Installationsverzeichnis, also etwa:  

```
cd /tmp/antivir-server-prof-<version>/bin
```

 ↳ In diesem Verzeichnis liegen die Dateien *antivir* und *antivir.asc*.
- ▶ Prüfen Sie die Unterschrift mit  

```
gpg --verify antivir.asc antivir
```

 ↳ Wenn Sie keine Fehlermeldungen erhalten, ist GnuPG bereit für Updates von AntiVir.
- ▶ Aktivieren Sie GnuPG für AntiVir. Tragen Sie hierfür in */etc/avupdater.conf* im Eintrag *GnuPGBinary* den vollen Pfad zur GnuPG-

Binärdatei ein, z. B.:

GnuPGBinary /usr/local/bin/gpg



Diese Option kann nur manuell in *avupdater.conf* editiert werden. Eine Einstellung über das Konfigurationsscript ist nicht möglich, um die Gefahr einer fehlerhaften Konfiguration zu mindern.

- ▶ Starten Sie den Internet Update Daemon neu, um die geänderten Einstellungen in *avupdater.conf* wirksam werden zu lassen:  
`/usr/lib/AntiVir/avupdater restart`

Die Authentizität der Updates wird ab jetzt durch GnuPG verifiziert.

## 4.6 AntiVir UNIX Server testen

Nach Abschluß der Installation und der Konfiguration können Sie die Funktionsfähigkeit von AntiVir testen. Hierfür ist ein Testvirus erhältlich. Dieser richtet keinerlei Schaden an, löst aber bei einem intakten Virenschutz auf Ihrem Rechner eine Reaktion des Programms aus.

### AntiVir mit Testvirus testen

- ▶ Wählen Sie in Ihrem Web-Browser die Adresse <http://www.eicar.org>.
- ▶ Informieren Sie sich auf dieser Webseite über den verfügbaren Testvirus *eicar.com*.
- ▶ Laden Sie den Testvirus auf Ihren Rechner.
  - ↳ Je nach Konfiguration von AntiVir und je nach Version des Testvirus blockiert der AntiVir Guard bereits das Abspeichern und löst eine Meldung aus.
- ▶ Versuchen Sie Zugriffe auf den Testvirus, z. B. durch Kopieren:  
`cp eicar.com eicar.com.txt`
  - ↳ Je nach Konfiguration von AntiVir blockiert der AntiVir Guard den Zugriff und führt eventuell weitere Aktionen aus wie Umbenennen oder Verschieben des Testvirus.

### Eventuelle Fehler suchen

Wenn der AntiVir Guard nicht die erwarteten Meldungen ausgibt oder Aktionen ausführt, müssen Sie Ihre Konfiguration überprüfen.

- ▶ Prüfen Sie, ob der AntiVir Guard läuft. Geben Sie ein:  
`/usr/lib/AntiVir/avguard status`
- ▶ Starten Sie den AntiVir Guard, falls nötig.
- ▶ Prüfen Sie in */etc/avguard.conf*, ob das Verzeichnis, in dem Sie arbeiten, in den überwachten Verzeichnissen liegt (siehe [Konfigurationsdatei avguard.conf](#) – Seite 34)
- ▶ Prüfen Sie in */etc/avguard.conf* den Wert von `AccessMask`. Wenn der Wert auf 0 gesetzt ist, ist der AntiVir Guard deaktiviert.
- ▶ Prüfen Sie Meldungen des AntiVir Guard an Ihre Logdatei oder an *syslog*, um den Fehler einzugrenzen.

## 5 Bedienung

Nach Abschluß der Installation und der Konfiguration ist die laufende Überwachung Ihres Systems durch AntiVir gewährleistet. Im laufenden Betrieb werden unter Umständen gelegentliche Änderungen der Konfiguration sinnvoll sein, die Sie gemäß [Konfiguration](#) – Seite 33 vornehmen.

Dennoch kann in bestimmten Fällen eine gezielte manuelle Suche nach Viren bzw. unerwünschten Programmen notwendig sein. Hierfür steht der AntiVir Kommandozeilenscanner zur Verfügung. Dieses Programm ermöglicht mit vielen Optionen spezifische Suchläufe.

Der AntiVir Kommandozeilenscanner kann in Skripte eingebunden werden und auch über Cron-Jobs regelmäßig ausgeführt werden. Dem fortgeschrittenen UNIX -Nutzer bieten sich damit zahllose Möglichkeiten einer optimal abgestimmten Überwachung seines Systems.

Dieses Kapitel ist unterteilt in folgende Abschnitte:

- In [AntiVir Kommandozeilenscanner im Überblick](#) – Seite 53 erhalten Sie einen Überblick über sämtliche Optionen des Kommandozeilenscanners.
- In [AntiVir Kommandozeilenscanner in der Anwendung](#) – Seite 58 werden exemplarische Anwendungen des Kommandozeilenscanners aufgeführt.
- In [Vorgehen bei Fund eines Virus/unerwünschten Programms](#) – Seite 61 geben wir einige Hinweise auf das, was Sie tun sollten, wenn AntiVir seine Arbeit verrichtet hat.

### 5.1 AntiVir Kommandozeilenscanner im Überblick

#### Aufruf

Der AntiVir Kommandozeilenscanner wird aufgerufen über

```
/usr/lib/AntiVir/antivir [-option] [Verzeichnis [...]]
```

Wenn bei der Installation, wie empfohlen, ein Link im Verzeichnis

```
/usr/bin
```

erstellt wurde, genügt auch der Aufruf

```
antivir [-option] [Verzeichnis [...]]
```

Wenn kein Verzeichnis angegeben wird, scannt der AntiVir Kommandozeilenscanner das aktuelle Verzeichnis.

Wenn gezielt Dateien in einem Verzeichnis durchsucht werden sollen, wird der AntiVir Kommandozeilenscanner aufgerufen über

```
antivir [-option] [Verzeichnis][Dateiname]
```

#### Optionen

Folgende Optionen stehen – auch kombinierbar – für den AntiVir Kommandozeilenscanner zur Verfügung:

| Option     | Funktion                                                                             |
|------------|--------------------------------------------------------------------------------------|
| --allfiles | Kurzform für --scan-mode=all<br>Bitte verwenden Sie künftig die --scan-mode= Option  |
| --alltypes | Kurzform für --with-alltypes<br>bitte verwenden Sie künftig die --with-<type> Option |

| Option                    | Funktion                                                                                                                                                                                                                                                                           |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --archive-max-count=N     | Schließt in Archiven enthaltene Dateien vom Scan aus, wenn mehr als die angegebene Anzahl von Dateien innerhalb einer Rekursionsstufe vorliegt                                                                                                                                     |
| --archive-max-size=N      | Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie beim Dekomprimieren größer als der angegebene Wert werden                                                                                                                                                           |
| --archive-max-ratio=N     | Schließt in Archiven enthaltene Dateien vom Scan aus, wenn sie einen Dekompressionsfaktor jenseits des angegebenen Wertes haben                                                                                                                                                    |
| --archive-max-recursion=N | Schließt in Archiven enthaltene Dateien vom Scan aus, wenn ihre Schachtelungstiefe größer als der angegebene Wert ist                                                                                                                                                              |
| -C <dateiname>            | Name der Konfigurationsdatei. Default: keine für on demand Scans, <i>/etc/avupdater.conf</i> für den Updater.                                                                                                                                                                      |
| --check                   | wird mit --update verwendet: AntiVir prüft, ob ein Update vorhanden ist. Falls vorhanden, gibt AntiVir eine entsprechende Meldung aus, führt das Update aber nicht aus                                                                                                             |
| -del                      | Bei einem Fund werden betroffene Dateien gelöscht                                                                                                                                                                                                                                  |
| -dmdas                    | Alle Makros eines Dokuments werden gelöscht, wenn eins verdächtig erscheint                                                                                                                                                                                                        |
| -dmdei                    | OLE-Dokumente mit verdächtigen Makros werden gelöscht                                                                                                                                                                                                                              |
| -dmse                     | Der Exit-Code von antivir wird auf 101 gesetzt, wenn ein Makro gefunden wird                                                                                                                                                                                                       |
| -e                        | Bei einem Fund werden betroffene Dateien (wenn möglich) repariert. Kann kombiniert werden mit:<br>-del um die Datei zu löschen,<br>-ren um die Datei umzubenennen<br>--moveto= um die Datei in ein Quarantäne-Verzeichnis zu verschieben, sollte die Reparatur nicht möglich sein. |
| --exclude=<name>          | Schließt das angegebene Verzeichnis oder die angegebene Datei vom Scan aus. Wildcards werden nicht unterstützt, statt dessen sind mehrere --exclude= Optionen anzugeben.                                                                                                           |
| --help                    | Alle möglichen Optionen werden ausgegeben                                                                                                                                                                                                                                          |
| --heur-macro              | Aktiviert die Heuristik für Makroviren in Dokumenten                                                                                                                                                                                                                               |
| --heur-nomacro            | Deaktiviert die Heuristik für Makroviren in Dokumenten                                                                                                                                                                                                                             |

| Option               | Funktion                                                                                                                                                                                          |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --heur-level=N       | Stellt die Erkennungsstufe der Win32-Datei-Heuristik ein.<br>Stufe 0: aus<br>Stufe 1: niedrig<br>Stufe 2: mittel<br>Stufe 3: hoch                                                                 |
| --home-dir=<dir>     | AntiVir sucht seine eigenen Dateien, z. B. antivir.vdf, in <dir>                                                                                                                                  |
| --info               | AntiVir gibt eine Liste der Namen von bekannten Viren, bekannter Malware sowie aller mit aufgenommenen unerwünschter Programme aus                                                                |
| -lang:DE<br>-lang:EN | AntiVir gibt deutsche bzw englische Texte aus (wenn für den einzelnen Aufruf gewünscht, normalerweise findet eine automatische Erkennung der im System eingestellten Sprache statt).              |
| --log-email=<addr>   | Sendet einen Report über diesen Scan-Durchlauf per Email an die angegebene Adresse (zusätzlich zur Ausgabe am Bildschirm)                                                                         |
| --moveto=<dir>       | Verschiebt betroffene Dateien in das angegebene Verzeichnis (eine sog. Quarantäne).                                                                                                               |
| -noboot              | Die Bootsektorprüfung wird abgeschaltet. Hiermit kann bei gezielten Suchläufe Zeit gespart werden, ansonsten wird die Option nicht empfohlen.                                                     |
| -nobreak             | Ctrl-C und Ctrl-Break werden deaktiviert. Hierdurch kann verhindert werden, dass ein Nutzer den Scanprozess abbricht.                                                                             |
| -nolnk               | Symbolische Links werden ignoriert                                                                                                                                                                |
| -nombr               | Die Master-Bootsektorprüfung wird abgeschaltet. Hiermit kann bei gezielten Suchläufe Zeit gespart werden, ansonsten wird die Option nicht empfohlen.                                              |
| -once                | AntiVir läuft nur einmal pro Tag: Mit dieser Option prüft AntiVir, ob es am gleichen Tag schon ausgeführt wurde. Wenn es bereits ausgeführt wurde, bricht es mit einer entsprechenden Meldung ab. |
| -onefs               | Links, die in ein anderes Dateisystem führen, werden ignoriert. Hierbei können Verzeichnisse von der Suche ausgelassen werden, die beispielsweise per NFS gemounted wurden.                       |
| -q                   | "Quiet": AntiVir unterdrückt alle Meldungen                                                                                                                                                       |
| -r1                  | Nur Funde von Viren und unerwünschten Programmen sowie Warnungen werden protokolliert                                                                                                             |
| -r2                  | Zusätzlich zu -r1 werden alle gescannten Verzeichnispfade protokolliert                                                                                                                           |

| Option               | Funktion                                                                                                                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r3                  | Alle gescannten Dateien werden protokolliert                                                                                                                                                                                                                                                   |
| -r4                  | Ausführliche Meldungen protokolliert                                                                                                                                                                                                                                                           |
| -ra                  | Die Logdatei wird an die bestehende Logdatei angehängt                                                                                                                                                                                                                                         |
| -ren                 | Bei einem Fund werden betroffene Dateien umbenannt                                                                                                                                                                                                                                             |
| -rf<dateiname>       | Die Logdatei wird mit dem Dateinamen <dateiname> erstellt. In <dateiname> können folgende Platzhalter verwendet werden:<br>-%d: Tag<br>-%m: Monat<br>-%y: Jahr                                                                                                                                 |
| -ro                  | Die Logdatei überschreibt die bestehende Logdatei                                                                                                                                                                                                                                              |
| -rs                  | Meldungen über Viren und unerwünschte Programme werden einzeilig ausgegeben                                                                                                                                                                                                                    |
| -s                   | Alle Unterverzeichnisse werden durchsucht                                                                                                                                                                                                                                                      |
| --scan-in-archive    | Auch Inhalte von gepackten Archiven werden gescannt                                                                                                                                                                                                                                            |
| --scan-in-mbox       | Auch Inhalte von Mailbox-Ordern werden gescannt.                                                                                                                                                                                                                                               |
| --scan-mode=<mode>   | Stellt das Verfahren ein, nach dem bestimmt wird, ob eine Datei zu scannen ist. <mode> kann all, smart oder extlist sein. smart ist die Voreinstellung für on demand Scan.                                                                                                                     |
| --temp=<dir>         | AntiVir legt seine temporären Dateien in <dir> ab                                                                                                                                                                                                                                              |
| --update             | AntiVir führt ein Update seiner eigenen Dateien durch, um den Schutz vor Viren und unerwünschten Programmen wieder auf den neuesten Stand zu bringen                                                                                                                                           |
| -v                   | Ein Intensiv-Scan wird durchgeführt. AntiVir prüft komplette Dateien. Möglicherweise werden hierbei auch Fehlmeldungen ausgegeben. Diese Option sollte nur im Ausnahmefall gewählt werden, z. B. nach einem Fund.                                                                              |
| --version            | Die Version von AntiVir wird angezeigt                                                                                                                                                                                                                                                         |
| --warnings-as-alerts | Behandelt nicht-fatale Situationen wie schwerwiegende Fehler. Beendet das Programm beim Auftreten von Warnungen mit dem gleichen Exit-Code wie beim Fund von Viren bzw. unerwünschten Programmen                                                                                               |
| --with-<type>        | Aktiviert die Erkennung von unerwünschten Programmen, die keine Viren sind. <type> kann eine der Varianten adspy, bdc, dial, game, heur-dblext, joke, pck, phish oder spr sein. Die Option kann mehrfach angegeben werden.<br>Die Abkürzung --with-alltypes aktiviert alle Typen gleichzeitig. |

| Option                              | Funktion                                                                                                                                                                                                                                                   |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--without-&lt;type&gt;</code> | Deaktiviert die Erkennung von unerwünschten Programmen, s.a. <code>--with-&lt;type&gt;</code>                                                                                                                                                              |
| <code>-z</code>                     | Synonym für <code>--scan-in-archive</code> . Bitte verwenden Sie künftig die <code>--scan-in-archive</code> Option.                                                                                                                                        |
| <code>@&lt;rspdatei&gt;</code>      | AntiVir liest Parameter aus der Datei <code>&lt;rspdatei&gt;</code> . In <code>&lt;rspdatei&gt;</code> muss jede Option in einer eigenen Zeile stehen. Hiermit lassen sich bestimmte Kombinationen von Parametern unter einem einprägsamen Namen aufrufen. |

### Exit-Codes

Der AntiVir Kommandozeilenscanner gibt nach der Ausführung Exit-Codes zurück. Diese können von fortgeschrittenen UNIX-Nutzern verwendet werden, um eigene Skripte zu erstellen.

| Exit-Code | Bedeutung                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------|
| 0         | Normales Programmende: kein Virus bzw. unerwünschtes Programm, kein Fehler                                        |
| 1         | Virus bzw. unerwünschtes Programm in Datei oder Bootsektor gefunden                                               |
| 2         | Virus bzw. unerwünschtes Programm im Speicher gefunden                                                            |
| 3         | Virus bzw. unerwünschtes Programm in Datei oder Bootsektor per Heuristik gefunden                                 |
| 100       | AntiVir hat nur den Hilfetext angezeigt                                                                           |
| 101       | Ein Makro wurde in einer Datei gefunden (bei Aufruf von AntiVir mit <code>-dmse</code> )                          |
| 102       | AntiVir startet nicht, weil der Parameter <code>-once</code> angegeben war und AntiVir bereits an diesem Tag lief |
| 200       | Programmabbruch wegen Speichermangel                                                                              |
| 201       | Die angegebene Responsedatei wurde nicht gefunden                                                                 |
| 202       | Innerhalb einer Responsedatei wurde eine weitere Responsedatei angegeben                                          |
| 203       | Ungültiger Parameter angegeben                                                                                    |
| 204       | Ungültiges Verzeichnis angegeben                                                                                  |
| 205       | Die angegebene Logdatei konnte nicht erzeugt werden                                                               |
| 210       | AntiVir hat eine benötigte DLL nicht gefunden                                                                     |
| 211       | Programm abgebrochen, da die Selbstprüfung fehlgeschlagen ist                                                     |
| 212       | Die Datei <i>antivir.vdf</i> konnte nicht gelesen werden                                                          |

| Exit-Code | Bedeutung                        |
|-----------|----------------------------------|
| 213       | Initialisierungsfehler           |
| 214       | Lizenzdatei wurde nicht gefunden |

In Verbindung mit `--update` hat der AntiVir Kommandozeilenscanner andere Exit Codes:

| Exit-Code | Bedeutung                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------|
| 0         | Kein Update erforderlich                                                                                            |
| 1         | AntiVir hat sich erfolgreich aktualisiert bzw., wenn <code>--check</code> angegeben wurde, ein Update ist verfügbar |
| >=2       | Update ist misslungen                                                                                               |

## 5.2 AntiVir Kommandozeilenscanner in der Anwendung

Dieser Abschnitt stellt häufige Anwendungen des AntiVir Kommandozeilenscanners vor.

Wenn der AntiVir Guard aktiv ist, werden durch die Verwendung des AntiVir Kommandozeilenscanner Dateien zweifach gescannt:

- Durch den AntiVir Guard, wenn die Datei durch den AntiVir Kommandozeilenscanner geöffnet wird
- Durch den AntiVir Kommandozeilenscanner selbst

Um störende Wechselwirkungen zu vermeiden, ist es also sinnvoll, den AntiVir Guard vorher zu deaktivieren über:

```
/usr/lib/AntiVir/avguard stop
```

Achten Sie darauf, dass Sie den AntiVir Guard nach dem Scan wieder starten mit:

```
/usr/lib/AntiVir/avguard start
```

### Kompletten Suchlauf durchführen

Nach der Installation ist es sinnvoll, einen kompletten Suchlauf über das Dateisystem durchzuführen. Ein solcher Suchlauf enthält sinnvollerweise folgende Optionen:

|                                |                                                               |
|--------------------------------|---------------------------------------------------------------|
| <code>--scan-mode=all</code>   | Scannt alle Dateien                                           |
| <code>--with-alltypes</code>   | Erkennt alle Arten von verdächtigen und unerwünschten Dateien |
| <code>-s</code>                | Scannt alle Unterverzeichnisse                                |
| <code>--scan-in-archive</code> | Scannt auch gepackte Dateien                                  |

► Geben Sie ein:

```
antivir --scan-mode=all --with-alltypes -s --scan-in-archive /
```

## Teilsuchlauf durchführen

In der Regel ist es ausreichend, diejenigen Verzeichnisse zu überprüfen, die ein- und ausgehende Daten enthalten (Mailbox, Internet, Text-Verzeichnis). Solche Daten liegen meist im Verzeichnis */var*.

Sind auf dem UNIX-System DOS-Partitionen vorhanden und gemounted, sollten diese auch geprüft werden.

Hier sind folgende Optionen sinnvoll:

|                                |                                |
|--------------------------------|--------------------------------|
| <code>--scan-mode=all</code>   | Scannt alle Dateien            |
| <code>-s</code>                | Scannt alle Unterverzeichnisse |
| <code>--scan-in-archive</code> | Scannt auch gepackte Dateien   |

Wenn Ihre DOS-Partitionen z. B. unter */mnt* und Ihre ein- und ausgehenden Daten unter */var* liegen:

► Geben Sie ein:

```
antivir --scan-mode=all -s --scan-in-archive /var /mnt
```

## Betroffene Dateien löschen

AntiVir kann Dateien löschen, die Viren oder unerwünschte Programme enthalten. Optional kann AntiVir vorher versuchen, die Dateien zu reparieren.

Beim Löschen werden die Dateien zunächst überschrieben und erst anschließend gelöscht. Sie lassen sich deshalb auch mit Reparatur-Tools nicht wiederherstellen.

Hier sind folgende Optionen sinnvoll:

|                              |                                                                           |
|------------------------------|---------------------------------------------------------------------------|
| <code>--scan-mode=all</code> | Scannt alle Dateien                                                       |
| <code>-del</code>            | Löscht betroffene Dateien                                                 |
| <code>-e -del</code>         | Versucht, betroffene Dateien zu reparieren und löscht irreparable Dateien |



In den nachfolgenden Beispielen werden Dateien umgewandelt oder gelöscht. Dabei kann wertvoller Datenbestand verloren gehen.

Beispiele Wenn Sie alle betroffenen Dateien in */home/myhome* löschen wollen:

► Geben Sie ein:

```
antivir --scan-mode=all -del /home/myhome
```

Wenn Sie betroffene Dateien in */home/myhome* reparieren und irreparable Dateien löschen wollen:

► Geben Sie ein:

```
antivir --scan-mode=all e -del /home/myhome
```

## AntiVir aufrufen, wenn es in einem anderen Verzeichnis als */usr/lib/AntiVir* installiert wurde

AntiVir benötigt für seinen Selbsttest die Information, in welchem Verzeichnis es installiert ist, wenn dieses nicht */usr/lib/AntiVir* ist.

Wenn AntiVir beispielsweise in */usr/local/AntiVir* installiert wurde:

- Geben Sie ein:

```
antivir --home-dir=/usr/local/AntiVir
```

### AntiVir manuell aktualisieren

AntiVir kann jederzeit manuell aktualisiert werden.

Es wird empfohlen, AntiVir zum Aktualisieren als **root** laufen zu lassen.

Vorteil: Eventuell laufende Prozesse der AntiVir-Daemons (z. B. den AntiVir Guard, SAVAPI Serverprozesse, AntiVir MailGate) werden automatisch mit den aktualisierten Virenschutzdateien geladen, ohne laufende Scanprozesse zu unterbrechen. Es ist also sichergestellt, dass alle Dateien gescannt werden.

Wenn AntiVir zum Aktualisieren nicht als **root** gestartet wird, besitzt es möglicherweise nicht die notwendigen Rechte, um alle AntiVir-Dämonen neu zu starten. Der Neustart muss dann manuell vorgenommen werden.

Wenn Sie AntiVir aktualisieren wollen:

- Geben Sie ein:

```
/usr/lib/AntiVir/antivir --update
```

Wenn Sie lediglich prüfen wollen, ob eine neue Version von AntiVir vorliegt, ohne AntiVir zu aktualisieren:

- Geben Sie ein:

```
/usr/lib/AntiVir/antivir --update --check
```

### AntiVir über ein Skript aktualisieren

Fortgeschrittene UNIX-Nutzer können den AntiVir Kommandozeilenscanner in ein Skript integrieren und die [Exit-Codes](#) – Seite 57 auswerten.

- Beispiel ► Schreiben Sie ein Skript in der folgenden Form, um die Meldungen von AntiVir zu unterdrücken und durch eigene zu ersetzen:

```
----- BEGIN SCRIPT -----
#!/bin/sh

/usr/lib/AntiVir/antivir --update -q
case $? in
 0)
 echo "AntiVir ist aktuell"
 ;;
 1)
 echo "AntiVir hat sich aktualisiert"
 ;;
 *)
 echo "Beim Aktualisieren ist ein Fehler aufgetreten"
 ;;
esac
----- END SCRIPT -----
```

## 5.3 Vorgehen bei Fund eines Virus/unerwünschten Programms

AntiVir hat bei richtiger Konfiguration alle wichtigen Aufgaben auf Ihrem Rechner bereits automatisch erledigt:

- Die betroffene Datei wurde repariert oder zumindest gesperrt.
- Wenn eine Reparatur nicht möglich war, wurde der Zugriff auf die Datei blockiert und die Datei, je nach Konfiguration, zusätzlich umbenannt oder verschoben. Die Gefahr einer Weitergabe des Virus oder unerwünschten Programms ist damit gebannt.

Folgende Schritte sollten Sie auf jeden Fall durchführen:

- ▶ Versuchen Sie zu ermitteln, auf welche Weise der Virus oder das unerwünschte Programm "eingeschleppt" wurde.
- ▶ Führen Sie gezielte Prüfungen an möglicherweise betroffenen Datenträgern durch.
- ▶ Informieren Sie Kollegen, Vorgesetzte oder Geschäftspartner.
- ▶ Informieren Sie Ihren Systemverantwortlichen, Ihren Viren- oder Datenschutzbeauftragten.

### Verdächtige Dateien an Avira GmbH schicken

- ▶ Senden Sie uns bitte Viren und unerwünschte Programme, die von unseren Produkten noch nicht erkannt oder entfernt werden können, zu. Das Gleiche gilt für sonstige verdächtige Dateien. Senden Sie uns den Virus oder das unerwünschte Programm gepackt (PGP, gzip, WinZIP, PKZip, Arj) im Anhang einer Email an [virus@avira.de](mailto:virus@avira.de).

Verwenden Sie beim Packen das Passwort **virus**. Die Datei kann dann nicht von eventuellen Virenscannern in den Email-Gateways gelöscht werden.



## 6 Grafische Benutzeroberfläche (GUI)

### 6.1 Übersicht

Die grafische Benutzeroberfläche (GUI) unterstützt Sie bei der Bedienung und Konfiguration von AntiVir UNIX Server und stellt den laufenden Überwachungsprozess grafisch dar. AntiVir UNIX Server ist aber auch ohne GUI voll funktionsfähig und vollständig konfigurierbar. Die GUI ist eine programmunabhängige Applikation. D. h., sie kann gestartet und gestoppt werden, ohne dass AntiVir UNIX Server beeinflusst wird.

Für die GUI benötigen Sie Sun Java 1.4.0 oder höher.

**Rechte** Mit der GUI kann man das Programm als normaler Benutzer steuern, es sind keine root-Rechte erforderlich.

Allerdings muss der Benutzer in der "antivir"-Gruppe sein, die bei der Installation angelegt wird.

► Dafür geben Sie ein (als root):

```
/usr/sbin/usermod -G group1,group2,group3,antivir username
```

group1 bis group3 sind dabei die Gruppen, zu denen ein Benutzer schon gehört, username ist der Name des Benutzers.

Um festzustellen, zu welchen Gruppen ein Benutzer gehört:

► Geben Sie ein:

```
/usr/bin/groups
```

**Starten** ► Starten Sie die GUI wie folgt:  
`antivir-gui`

Falls mit diesem Befehl die Java-Installation nicht gefunden wird:

► Erstellen Sie einen soft-link in `/usr/bin` (als root):

```
ln -s /PFAD/ZUR/JAVA/INSTALLATION/bin/java /usr/bin
```

**Kommunikation** Die GUI kommuniziert mit AntiVir UNIX Server mit SSL über das Loopback Netzwerk Interface. Folgende Parameter müssen in der Konfigurationsdatei *avguard.conf* eingetragen sein:

```
GuiSupport yes
```

```
GuiCAFile /usr/lib/AntiVir/gui/cert/cacert.pem
```

```
GuiCertFile /usr/lib/AntiVir/gui/cert/server.pem
```

```
GuiCertPass antivir_default
```

Wenn diese Parameter nicht vorhanden oder falsch sind, steht die GUI nicht zur Verfügung. Mögliche Fehler werden in der log-Datei protokolliert.

**Mehrere Produkte** Sind mehrere AntiVir-Produkte auf einem Computer installiert, werden diese in der GUI mit je einem Reiter gezeigt. Damit können Sie die einzelnen Produkte leicht überwachen und konfigurieren. Je nachdem, welchen Reiter Sie anklicken, erscheinen die produktspezifischen GUIs und Menüs.

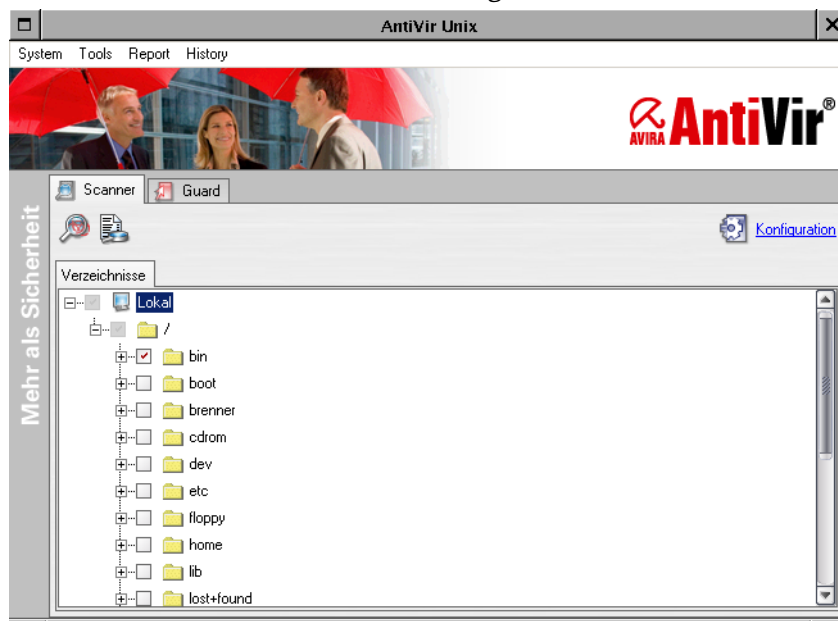
- Probleme Prüfen Sie bei Problemen mit der GUI, ob folgende Bedingungen erfüllt sind:
- AntiVir UNIX Server muss in `/usr/lib/AntiVir` installiert sein.
  - Es muss eine gültige Lizenz für AntiVir UNIX Server vorhanden sein (`antivir --version`).
  - In der Datei `avguard.conf` muss der Parameter für `GuiSupport` gesetzt sein.
  - Der Benutzer muss in der "antivir"-Gruppe sein.
- Sind diese Bedingungen nicht erfüllt, erscheint eine entsprechende Meldung.

## 6.2 AntiVir Scanner

### 6.2.1 AntiVir Scanner über GUI bedienen

#### GUI starten

- ▶ Starten Sie die GUI:  
`/usr/lib/AntiVir/antivir-gui`
- ↳ Die GUI erscheint mit dem Dialogfenster **Verzeichnisse**.



#### Symboleiste



Anklicken schaltet in das Dialogfenster des Scanvorgangs und startet diesen.



Anklicken schaltet das Dialogfenster **Log** um.



Anklicken öffnet das Dialogfenster **Konfiguration**.

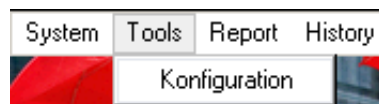
## Menüleiste

System



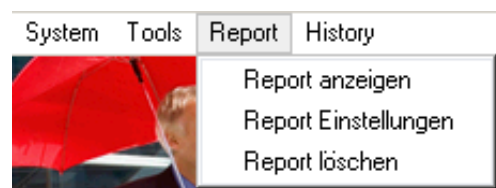
- **Netzwerk-Browser:** Zum Auswählen anderer Computer im Netzwerk, auf denen die GUI des Scanners läuft
- **Zertifikate verwalten:** Zum Verwalten bereits integrierter Zertifikate anderer Computer (für künftige Versionen vorgesehen)
- **Über...:** Informationen über die GUI
- **Beenden:** Schließt die GUI. AntiVir UNIX Server selbst wird nicht beendet.

Tools



- **Konfiguration:** Öffnet das Dialogfenster **Konfiguration**

Report



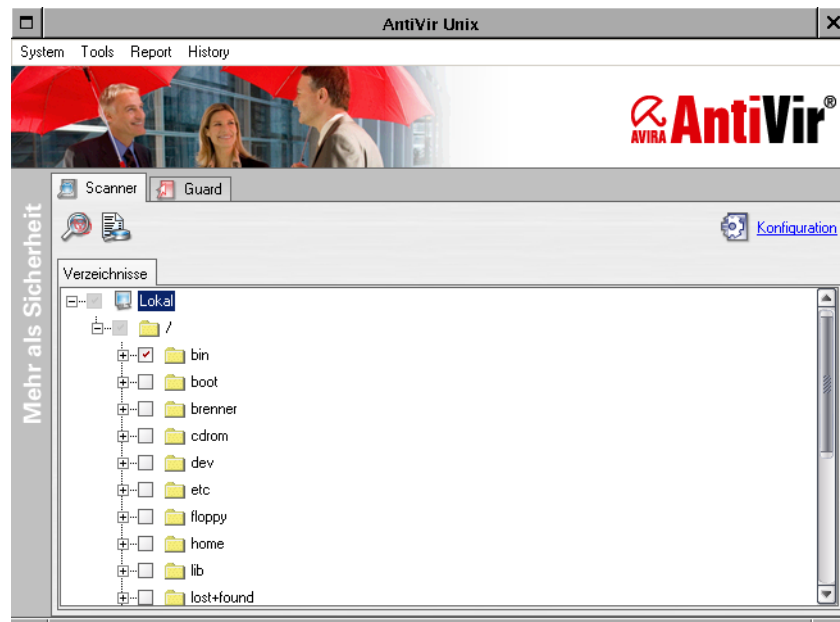
- **Report anzeigen:** Öffnet ein Dialogfenster, in dem der Inhalt der Reportdatei angezeigt wird (*avscanner.log*)
- **Report Einstellungen:** Öffnet das Dialogfenster **Konfiguration**, Bereich **Report**
- **Report löschen:** Löscht die im Bereich **Report** des Konfigurationsdialogs angegebene Reportdatei

History



- **Kurzreport anzeigen:** Öffnet das Dialogfenster **Kurzreport**
- **Kurzreport Einstellungen:** Öffnet das Dialogfenster **Konfiguration**, Bereich **Kurzreport**
- **Kurzreport löschen:** Löscht die im Bereich **Report** des Konfigurationsdialogs angegebene Kurzreportdatei

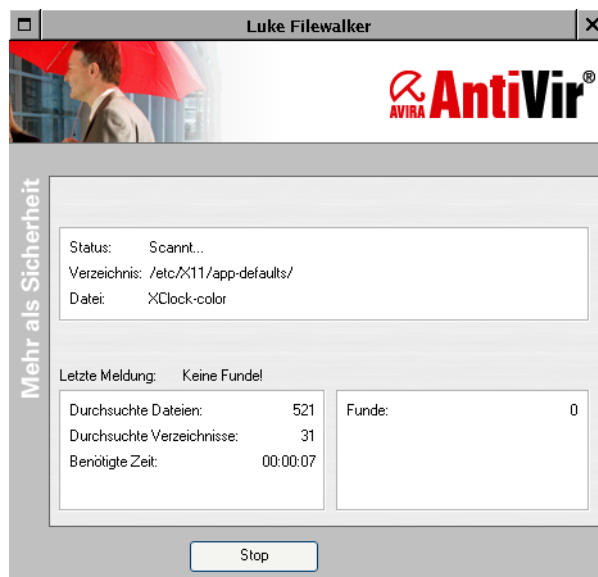
## Scanvorgang starten



- ▶ Wählen Sie im Dialogfenster **Verzeichnisse** die gewünschten Computer, Ordner und Dateien durch Klicken auf die davorstehenden Kontrollkästchen.
- ▶ Klicken Sie auf das Symbol mit der Lupe.
  - ↳ Das Dialogfenster des Scanvorgangs erscheint. Der Scanner durchsucht die gewählten Bereiche mit der aktuellen Konfiguration.



Alle Computer müssen die ausführbare Datei *antivir* in dem Verzeichnis haben, das in der Konfiguration angegeben wurde.



Status    Anzeige des Status

Verzeichnis    aktuell gescanntes Verzeichnis

Datei    aktuell gescannte Datei

|                           |                                                                   |
|---------------------------|-------------------------------------------------------------------|
| Letzte Meldung            | Anzeige des zuletzt gefundenen Virus bzw. unerwünschten Programms |
| Durchsuchte Dateien       | Anzahl aller gescannten Dateien                                   |
| Durchsuchte Verzeichnisse | Anzahl aller Verzeichnisse in denen gescannt wurde                |
| Benötigte Zeit            | Dauer des Suchvorgangs                                            |
| Funde                     | Anzeige der aktuellen Alarme                                      |

### Scanvorgang stoppen

Über die Schaltfläche **Stop** kann der aktuelle Scanprozess beendet werden. Diese Schaltfläche ist nur aktiv, wenn im Dialogfenster **Konfiguration/Suchen** das Kontrollkästchen **Stoppen zulassen** aktiviert ist.

- Klicken Sie auf die Schaltfläche **Stop**.
  - ↳ Der Scanvorgang wird beendet.

### Kurzreport anzeigen

- Klicken Sie in der Menüleiste **History/Kurzreport anzeigen....**
  - ↳ Das Dialogfenster **Kurzreport** erscheint:



Jeder Scanvorgang erhält einen Kurzreport.

Ein Hauptknoten besteht aus Datum und Uhrzeit, einem blauen Haken (kein Virus bzw. unerwünschtes Programm entdeckt) oder einem roten Pfeil (Virus bzw. unerwünschtes Programm entdeckt).

Am Ende des Hauptknotens können folgende Symbole erscheinen:

|   |                                          |
|---|------------------------------------------|
| * | Suche durch Benutzer abgebrochen         |
| # | Suche durch belegten Scanner abgebrochen |
| + | Suche durch Offlinerechner abgebrochen   |

Wird ein Hauptknoten aufgeklappt, erscheinen folgende Informationen:

- Details des Suchlaufs vom <Datum> <Uhrzeit>
- Meldung zur Beendigung der Suche
- Benötigte Suchzeit
- Anzahl der durchsuchten Verzeichnisse

- Anzahl der durchsuchten Dateien
- Anzahl der Warnungen, die vom Scanner geliefert wurden
- Anzahl der gelöschten Dateien
- Anzahl der reparierten Dateien
- Anzahl der Funde (Alerts) vom Kommandozeilenscanner
- Bezeichnung des letzten Fundes (z. B. Eicar-Test-Signatur)

Wenn Sie das Dialogfenster **Kurzreport** schließen wollen:

- ▶ Klicken Sie auf **Schließen**.
  - ↳ Das Dialogfenster wird geschlossen.

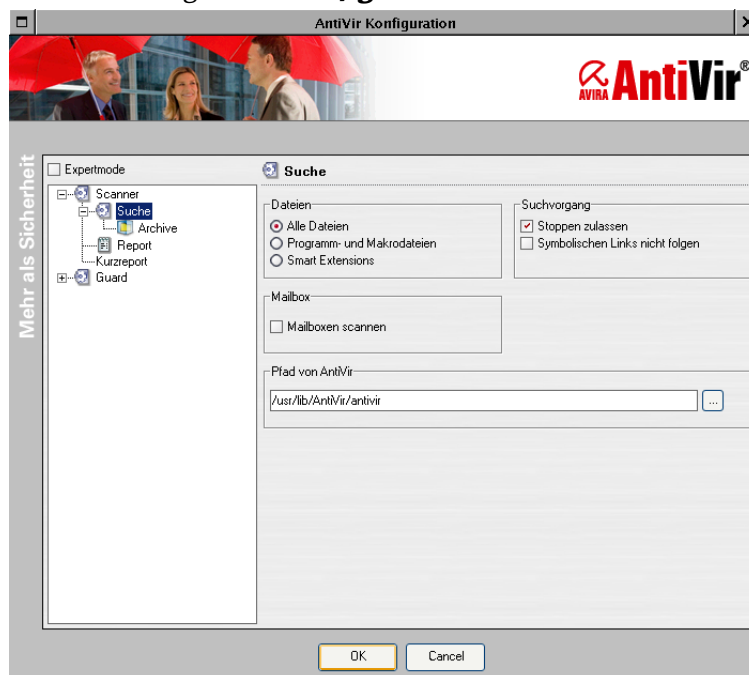
Wenn Sie die Kurzreports löschen wollen:

- ▶ Klicken Sie auf **Löschen**.
  - ↳ Es werden alle Kurzreports gelöscht.

### 6.2.2 AntiVir Scanner über GUI konfigurieren



- ▶ Klicken Sie auf das Symbol für **Konfiguration** in der Symbolleiste.
  - ODER –
- Klicken Sie in der Menüleiste auf **Tools/Konfigurationsmenü**.
  - ↳ Das Dialogfenster **Konfiguration** erscheint:



Bei der Konfiguration wird unterschieden zwischen "Grundeinstellungen" und "Experteneinstellungen". Für letztere muss das Optionsfeld **Expertmode** aktiviert sein.

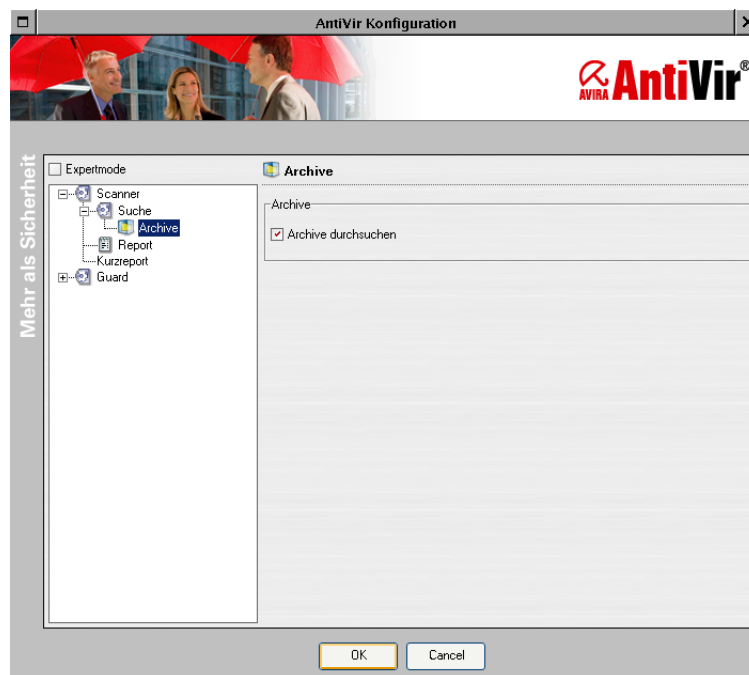
- ▶ Klicken Sie in der Baumstruktur auf einen Eintrag.
  - ↳ Ein Dialogfenster mit den Einstellungen für den jeweiligen Bereich erscheint.

## Grundeinstellungen - Bereich Suchen

Hier legen Sie das grundlegende Verhalten der Suchroutine fest.

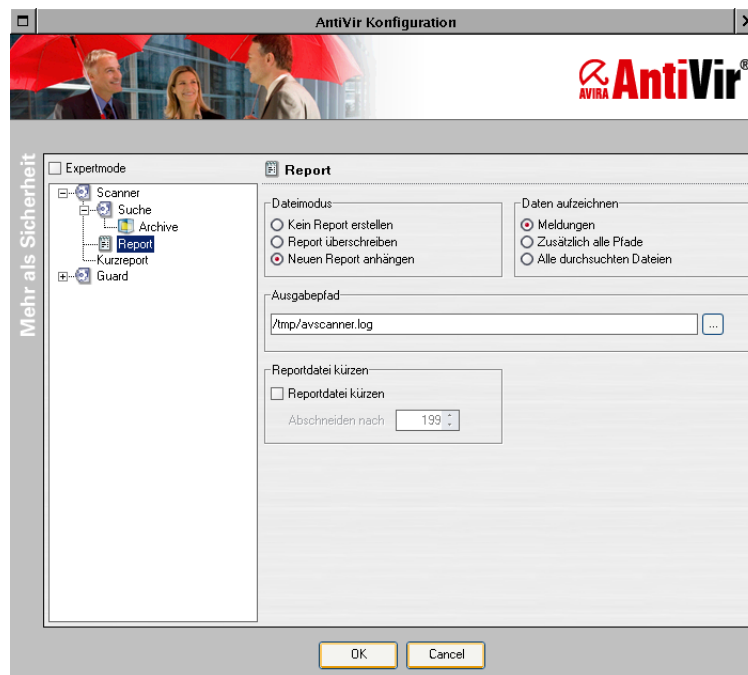
- Dateien Je nachdem, ob alle Dateien, Programm- und Makrodateien oder Smart (nähere Info unter Scanmode) gescannt werden sollen:
- ▶ Aktivieren Sie das entsprechende Optionsfeld.
- Mailbox Wenn die Inhalte Ihrer Mailboxen gescannt werden sollen:
- ▶ Aktivieren Sie das Kontrollkästchen **Mailboxen scannen**.
- Pfad von AntiVir Im Eingabefeld **Pfad von AntiVir** befindet sich der Pfad, in dem AntiVir installiert wurde. In der Regel liegt die Programmdatei in:
- ```
/usr/lib/AntiVir/antivir
```
- Suchvorgang
- ▶ Wenn Sie einen manuellen Abbruch des Suchvorgangs zulassen wollen:
 - ↳ Aktivieren Sie das Kontrollkästchen **Stoppen zulassen**.
 - ▶ Wenn Sie symbolischen Links beim Scannen nicht folgen möchten:
 - ↳ Aktivieren Sie das Kontrollkästchen **Symbolischen Links nicht folgen**.

Grundeinstellungen - Bereich Archive



- Archive Wenn Archive durchsucht werden sollen:
- ▶ Aktivieren Sie das Kontrollkästchen **Archive durchsuchen**.

Grundeinstellungen - Bereich Report



Dateimodus Die Meldungen des Kommandozeilenscanners werden in einer Reportdatei gesammelt. Folgende Optionen stehen Ihnen zur Verfügung:

- Keinen Report erstellen
 - Report überschreiben
 - Neuen Report anhängen
- Aktivieren Sie das entsprechende Optionsfeld.

Datei aufzeichnen Sie können verschiedene Daten in der Reportdatei sammeln. Diese wären:

- Meldungen
- zusätzliche Pfade
- alle durchsuchten Dateien

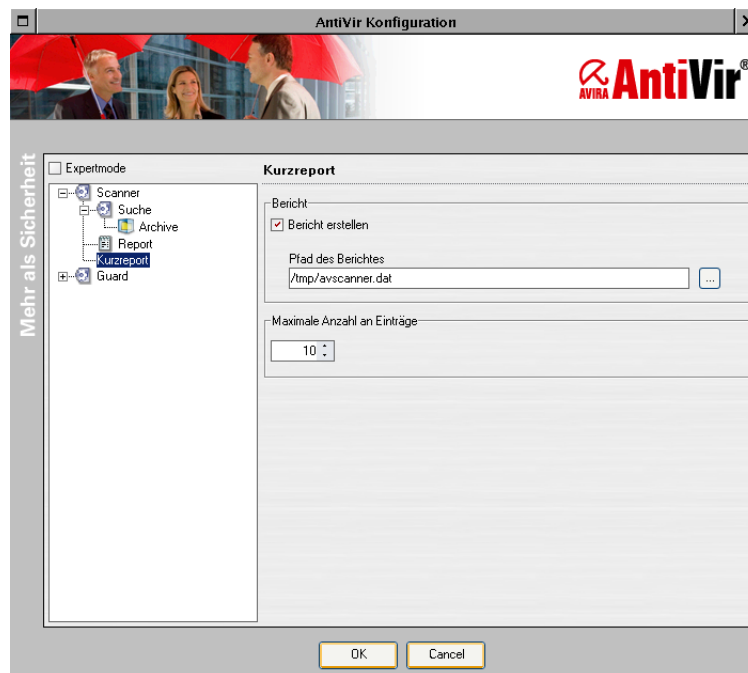
Die zweite Option schließt die erste ein und die dritte schließt die ersten beiden ein.

► Aktivieren Sie das entsprechende Optionsfeld.

Ausgabepfad ► Geben Sie ggf. den Pfad der Reportdatei an, z. B.:
/home/username/.AntiVir/avscanner.log

Reportdatei kürzen ► Aktivieren Sie das Kontrollkästchen **Reportdatei kürzen** um die maximale Größe für die Reportdatei festzulegen.

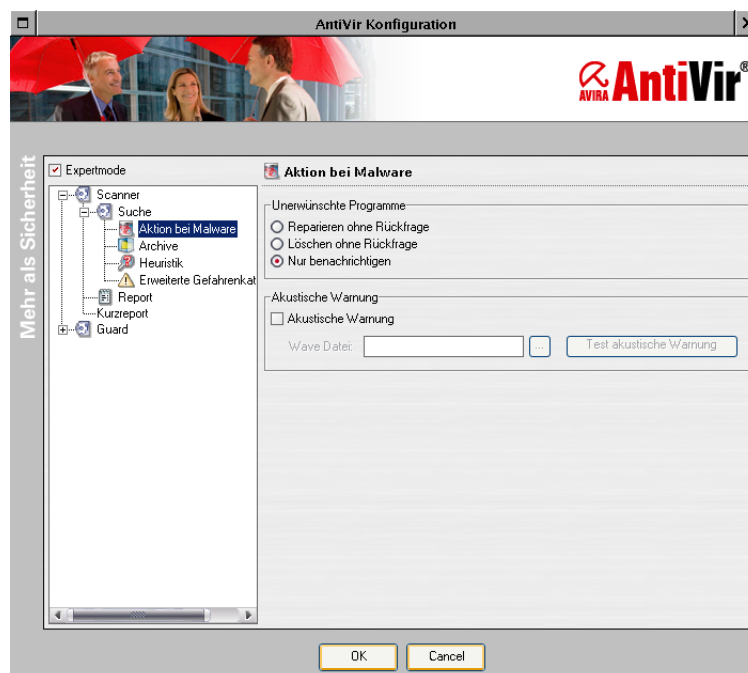
Grundeinstellungen - Bereich Kurzreport



Bericht Wenn ein Kurzreport angelegt werden soll:

- ▶ Aktivieren Sie das Kontrollkästchen **Kurzreport erstellen**.
- ▶ Geben Sie den Pfad der Kurzreportdatei an.
- ▶ Legen Sie die Anzahl der Einträge fest.

Experteneinstellungen - Bereich Aktion bei Malware



Unerwünschte
Programme

Legt fest wie bei einem Malware Fund vorgegangen wird:

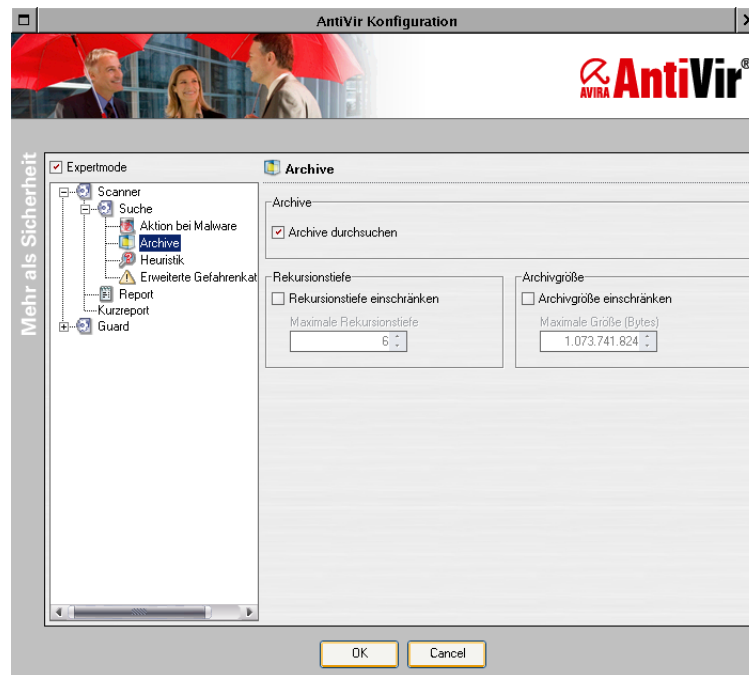
- **Reparieren ohne Rückfrage** - versucht die betroffene Datei automatisch zu reparieren.

- **Löschen ohne Rückfrage** - löscht die betroffene Datei
 - **Nur benachrichtigen**
- Aktivieren Sie das entsprechende Optionsfeld.

Akustische
Warnung

- Aktivieren Sie das Kontrollkästchen **Akustische Warnung** um die *.wav Datei bei einem Fund abzuspielen.

Experteneinstellungen - Bereich Archive



Im Expertenmodus haben Sie zusätzlich noch die Möglichkeit folgendes einzustellen:

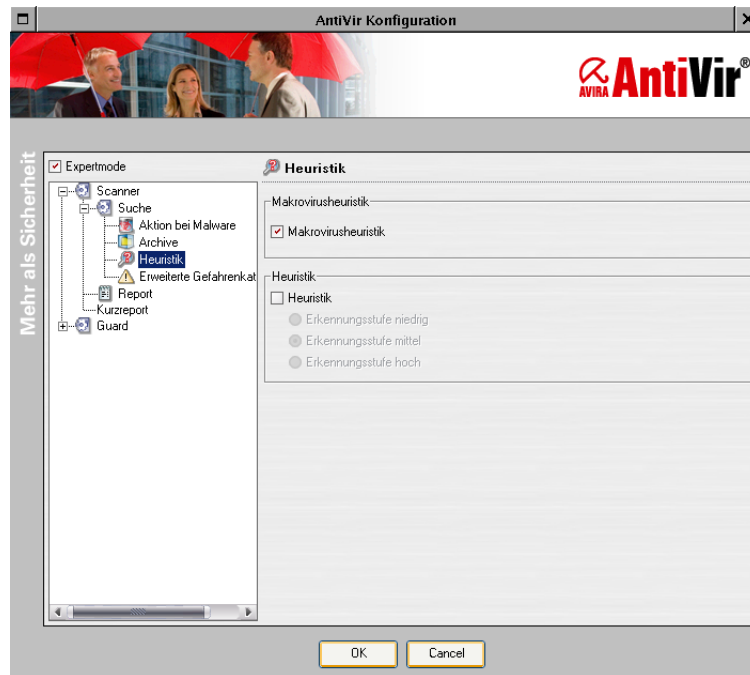
Rekursionstiefe

- Aktivieren Sie das Kontrollkästchen **Rekursionstiefe einschränken**, um die **Maximale Rekursionstiefe** für ein Archiv festzulegen.

Archivgröße

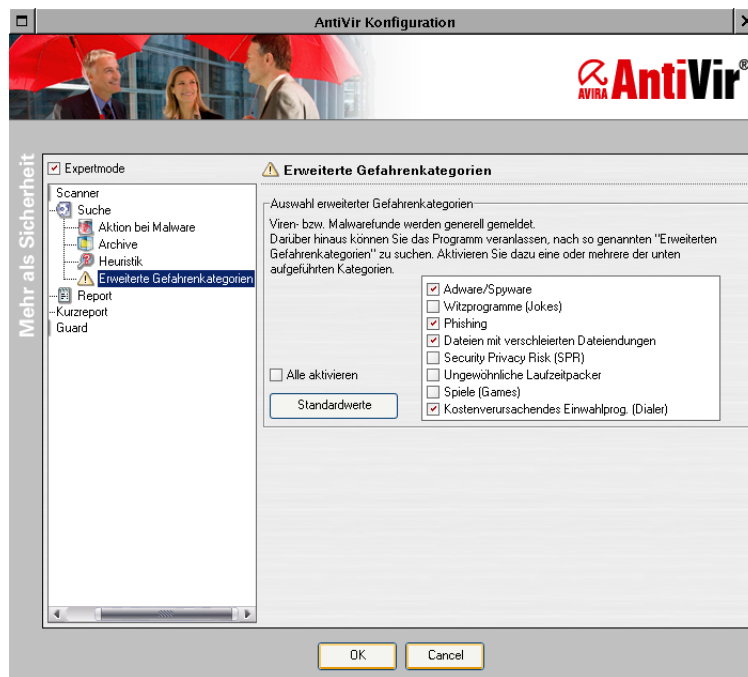
- Aktivieren Sie das Kontrollkästchen **Archivgröße einschränken**, um die **Maximale Archivgröße** für ein Archiv festzulegen.

Experteneinstellungen - Bereich Heuristik



- Makrovirus-
heuristik ► Aktivieren Sie das Kontrollkästchen **Makrovirusheuristik**, um die **Heuristik für Makroviren** in Dokumenten einzuschalten.
- Heuristik ► Aktivieren Sie das Kontrollkästchen **Heuristik**, um die **Win32-Datei-Heuristik** einzustellen, die auch unbekannte Dateiviren, Würmer, Trojaner etc. entdecken kann. Sie können einstellen, wie aggressiv diese Heuristik sein soll:
- Erkennungsstufe niedrig
 - Erkennungsstufe mittel
 - Erkennungsstufe hoch

Experteneinstellungen - Bereich Erweiterte Gefahrenkategorien



Erweiterte
Gefahren-
kategorien

- ▶ Sie können AntiVir dazu veranlassen, nach so genannten **Erweiterten Gefahrenkategorien** zu suchen. Aktivieren Sie dazu eine oder mehrere der aufgeführten Kategorien.
- ▶ Für eine nähere Beschreibung lesen Sie bitte den "Tooltip".
- ▶ Die Liste kann sich nach einem Update ändern.

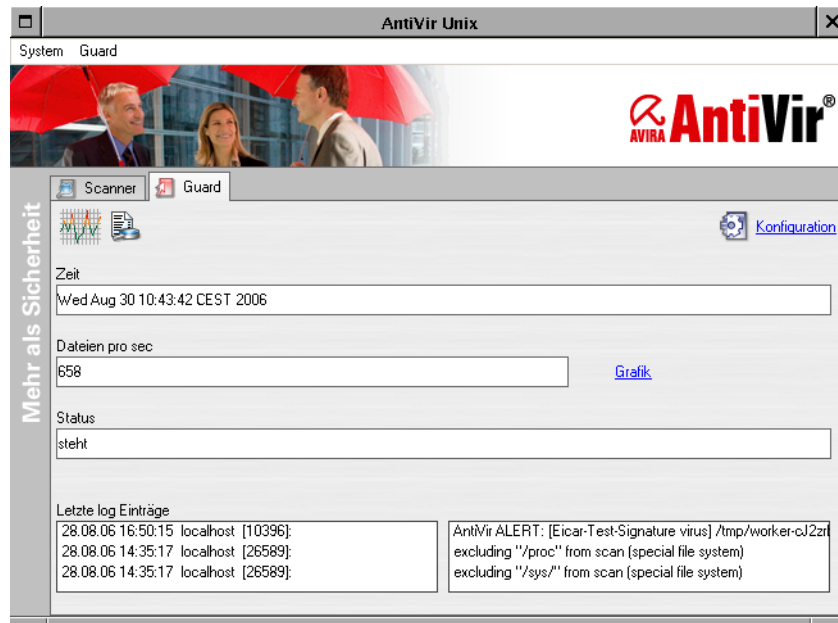
6.3 AntiVir Guard

6.3.1 AntiVir Guard über GUI bedienen

GUI starten

- ✓ Damit AntiVir Guard mit der GUI kommuniziert, muss der Eintrag GuiSupport in *avguard.conf* aktiviert sein.
- ▶ Starten Sie die GUI:
`/usr/lib/AntiVir/antivir-gui`
 - ↳ Die GUI erscheint mit dem Dialogfenster **Verzeichnisse**.

► Klicken Sie auf den Reiter **Guard**.



Symbolleiste



Anklicken schaltet in das Dialogfenster **Echtzeit Status** um



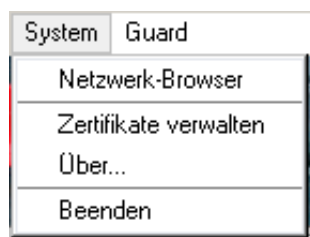
Anklicken schaltet in das Dialogfenster **Log Datei** um



Anklicken schaltet in das Dialogfenster **Konfiguration** um

Menüleiste

System



- **Netzwerk-Browser:** Zum Auswählen anderer Computer im Netzwerk, auf denen die GUI des AntiVir Guard läuft
- **Zertifikate verwalten:** Zum Verwalten bereits integrierter Zertifikate anderer Computer (für künftige Versionen vorgesehen)
- **Über...** : Informationen über die GUI
- **Beenden:** Schließt die GUI. AntiVir Guard selbst wird nicht beendet

Guard



- **Echtzeit:** Schaltet in das Dialogfenster **Echtzeit** um
- **Log:** Schaltet in das Dialogfenster **Log Datei** um
- **Konfiguration:** Öffnet das Dialogfenster **Konfiguration**
- **Konfiguration laden:** Lädt eine bereits gespeicherte Konfiguration
- **Konfiguration speichern:** Speichert die aktuelle Konfiguration
- **Start Guard:** Startet den AntiVir Guard
- **Stop Guard:** Stoppt den AntiVir Guard

Dialogfenster Echtzeit Status

Abbildung siehe [GUI starten](#) – Seite 64

Im Dialogfenster **Echtzeit Status** werden die aktuellen Dateizugriffe angezeigt, z. B. 286 Dateien/Sekunde. Außerdem werden der aktuelle Status des AntiVir Guards und die letzten Einträge in das Log angezeigt.

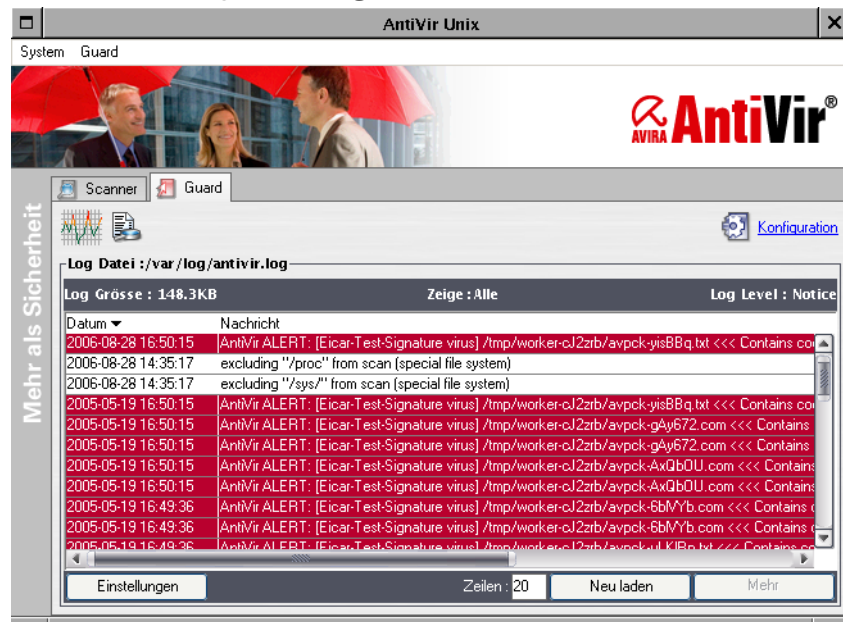
Status anzeigen In der Ecke rechts oben des Dialogfensters wird der aktuelle Status des AntiVir Guards angezeigt (**steht/läuft**).

Dialogfenster Logdatei



- Klicken Sie in der Symbolleiste auf die Schaltfläche für Logdatei.
– ODER –
Wählen Sie den Menüeintrag **Guard/Log Datei**.

↳ Das Dialogfenster **Log Datei** erscheint:

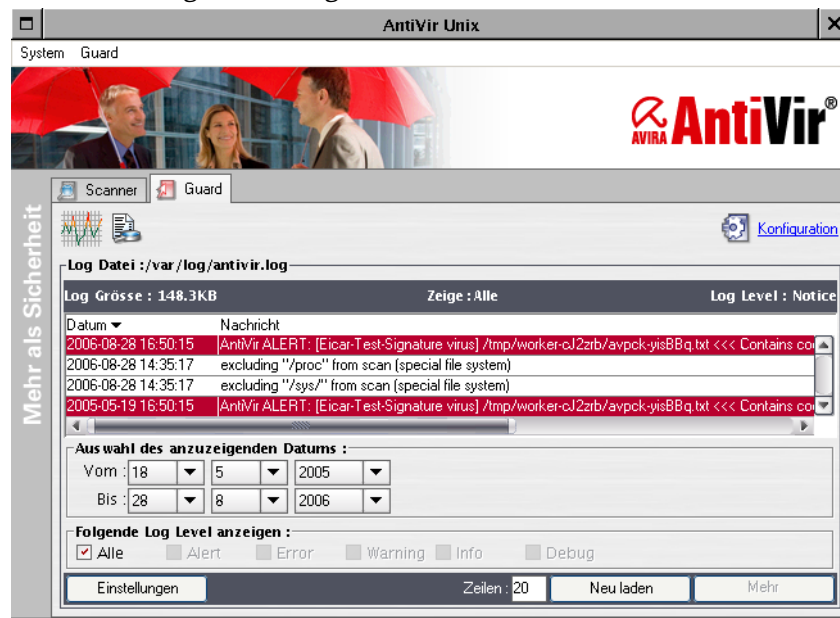


Log Datei Zeigt die komplette Logdatei mit Angabe des Pfads an, darunter die aktuelle Größe der Logdatei in KB, welche Log Level angezeigt werden und welchen Log Level der AntiVir Guard verwendet.

Unter dem Ausgabefenster befinden sich vier Schaltflächen: **Einstellungen**, **Zeilen**, **Neu laden** und **Mehr**:

Einstellungen ► Klicken Sie auf die Schaltfläche **Einstellungen**.

↳ Das folgende Dialogfenster erscheint:



- **Auswahl des anzuzeigenden Datums:** Auswahl des Zeitfensters, in dem Einträge der Logdatei angezeigt werden sollen; Standardeinstellung: komplette Logdatei.
- **Folgende Log Level anzeigen:** Auswahl der anzuzeigenden Log Level; Standardeinstellung: **Alle**

- Zeilen Anzahl der zu ladenden Logzeilen
- Neu laden Logdatei neu laden
- Mehr Bei geladener Logdatei wird die Ansicht um die bei **Zeilen** angegebene Anzahl erweitert.

Dialogfenster Konfiguration

siehe [AntiVir Guard über GUI konfigurieren](#) – Seite 78

AntiVir Guard starten und beenden

- Starten ► Wählen Sie den Menüeintrag **Guard/Start Guard**.
- Beenden ► Wählen Sie den Menüeintrag **Guard/Stop Guard**.

GUI beenden

- Wählen Sie den Menüeintrag **System/Beenden**.
↳ Die GUI wird beendet.



Wenn Sie die GUI beenden, bleibt der aktuelle Status des AntiVir Guard erhalten.

6.3.2 AntiVir Guard über GUI konfigurieren

Sie können die Parameter aus der Konfigurationsdatei *avguard.conf* über die GUI anpassen.

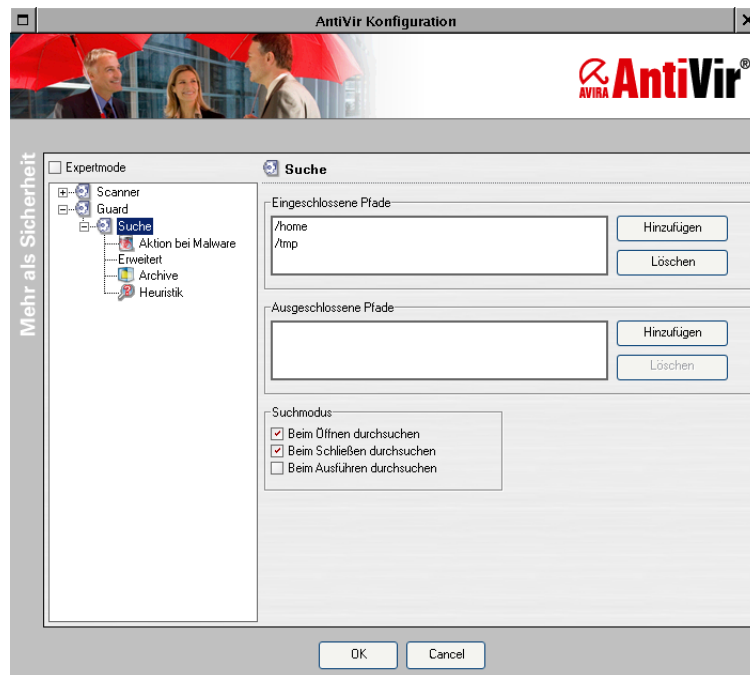
Zum besseren Verständnis wird für jeden Parameter der entsprechende Eintrag in *avguard.conf* aufgeführt. Die Parameter sind im Kapitel [Konfigurationsdateien](#) – Seite 34 ausführlich beschrieben.

Dialogfenster Konfiguration öffnen



- Klicken Sie auf das Symbol für Konfiguration in der Symbolleiste.
– ODER –
Wählen Sie den Menüeintrag **Guard/Konfiguration**.

- ↳ Das Dialogfenster **Konfiguration** mit den Grundeinstellungen von AntiVir Guard erscheint:



Bei der Konfiguration wird unterschieden zwischen "Grundeinstellungen" und "Experteneinstellungen". Für letztere muss das Optionsfeld **Expertmode** aktiviert sein.

- ▶ Wählen Sie in der Baumstruktur einen Eintrag.
 - ↳ Ein Dialogfenster mit den Einstellungen für den jeweiligen Bereich erscheint.

Grundeinstellungen - Bereich Suche

Eingeschlossene Pfade Der AntiVir Guard scannt die Dateien im angegebenen Verzeichnis inklusive aller Unterverzeichnisse.

Die Daten der verschiedenen Nutzer liegen üblicherweise unter */home*.

Pro Eintrag ist nur ein Verzeichnis zugelassen. Mehrere Verzeichnisse können angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile.

Beispiel: */home* und */var*.

Wenn kein Verzeichnis angegeben wird, überwacht der AntiVir Guard keine Dateien! Hierdurch wird `IncludePath` in `avguard.conf` gesetzt.

- ▶ Klicken Sie auf **Hinzufügen**.

↳ Das Dialogfenster **New path** erscheint.

- ▶ Geben Sie den Pfad des gewünschten Verzeichnisses ein, klicken Sie auf **Add** und bestätigen Sie mit **OK**.

Wenn Sie ein Verzeichnis aus der Liste entfernen wollen:

- ▶ Wählen Sie das gewünschte Verzeichnis und klicken Sie auf **Löschen**.

Ausgeschlossene Pfade Ausgeschlossene Verzeichnisse:
Der AntiVir Guard kann einzelne Verzeichnisse von der Überwachung ausnehmen, z. B. ein Verzeichnis, in das temporäre Dateien von AntiVir-Komponenten gelegt werden. Eine Voreinstellung gibt es nicht.

Pro Eintrag ist nur ein Verzeichnis zugelassen. Mehrere Verzeichnisse können angegeben werden, allerdings jeweils als eigener Eintrag in einer separaten Zeile.

Beispiel: `/home/log` und `/home/tmp`

Wenn Sie **Verschieben nach** im Bereich **Unerwünschtes** gewählt haben, wird dieses Verzeichnis automatisch auch als ausgeschlossenes Verzeichnis interpretiert.

Hierdurch wird `ExcludePath` in `avguard.conf` gesetzt.

► Klicken Sie auf **Hinzufügen**.

↳ Das Dialogfenster **New path** erscheint.

► Geben Sie den Pfad des gewünschten Verzeichnisses ein, klicken Sie auf **Add** und bestätigen Sie mit **OK**.

Wenn Sie ein Verzeichnis aus der Liste entfernen wollen:

► Wählen Sie das gewünschte Verzeichnis und klicken Sie auf **Löschen**.

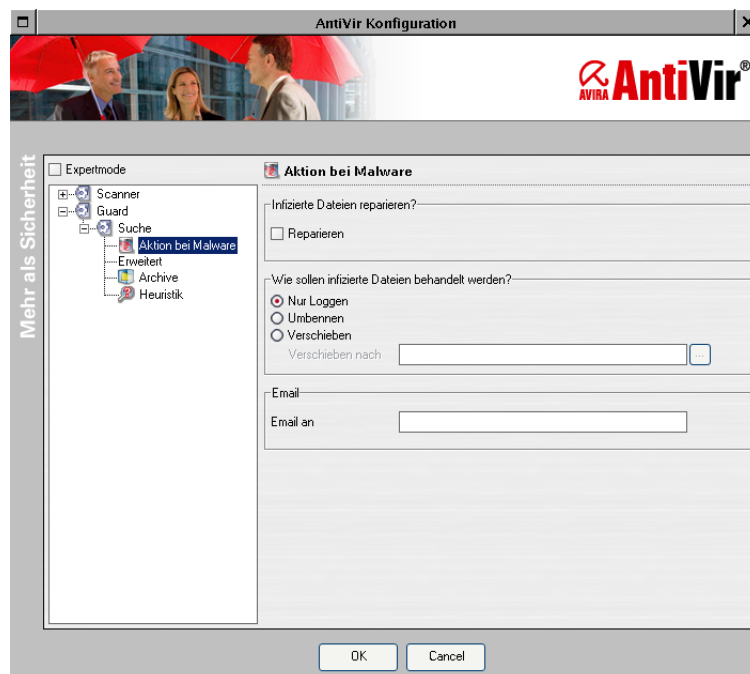
Suschmodus Hier wird festgelegt, bei welchen Zugriffen der AntiVir Guard eine Datei auf Viren und unerwünschte Programme durchsucht:

- Scannen beim Öffnen einer Datei
- Scannen beim Schließen einer Datei
- Scannen beim Ausführen einer Datei

Hierdurch wird `AccessMask` in `avguard.conf` gesetzt.

► Aktivieren Sie das (die) gewünschte(n) Kontrollkästchen.

Grundeinstellungen - Bereich Aktion bei Malware



Infizierte Dateien reparieren Der AntiVir Guard ist in der Lage, Dateien sofort beim Zugriff zu reparieren. Schlägt dies fehl, wird der Zugriff geblockt. In der Voreinstellung ist diese Option deaktiviert.

Hierdurch wird `RepairConcerningFiles` in `avguard.conf` gesetzt.

► Aktivieren Sie ggf. das Kontrollkästchen **Reparieren**.

Wie sollen betroffene Dateien behandelt werden?

Wenn das Kontrollkästchen **Reparieren** deaktiviert oder die Reparatur nicht möglich ist, wird der Zugriff auf die Datei gesperrt und der Vorgang protokolliert. Über folgende drei Optionen werden weitere Aktionen vom AntiVir Guard definiert:

- Nur Loggen: keine weiteren Aktionen
- Umbenennen: Umbenennen der Datei durch Anhängen der Endung .XXX
- Verschieben: Verschieben der Datei in ein beliebiges auszuwählendes Verzeichnis. Dieses Verzeichnis wird automatisch angelegt, wenn es noch nicht existiert.
Beispiel: /home/unwanted

Hierdurch werden LogOnly, RenameConcerningFiles und MoveConcerningFilesTo in *avguard.conf* gesetzt.

► Wählen Sie das gewünschte Optionsfeld.

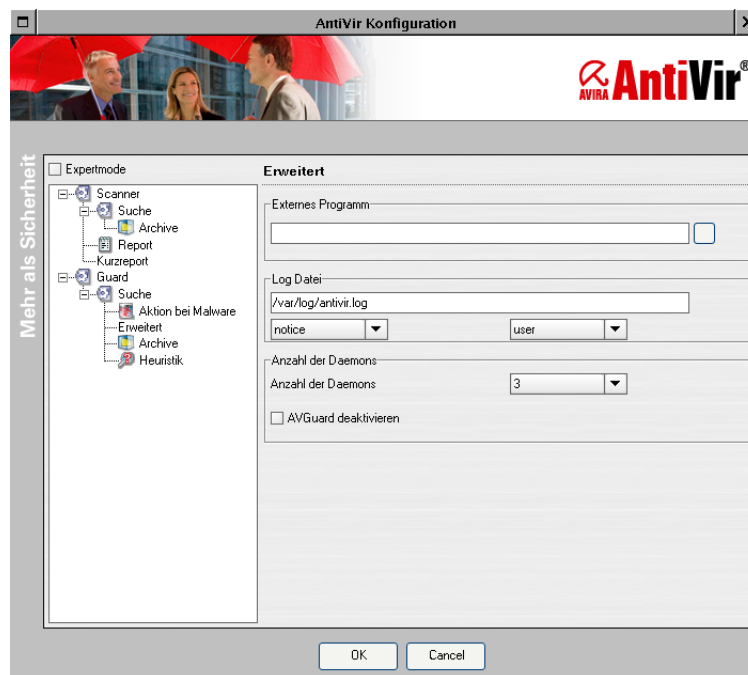
Wenn Sie die Option **Verschieben** gewählt haben:

► Geben Sie ein Verzeichnis an, in das die betroffene Datei verschoben werden soll.

Email Soll beim Fund eines Virus bzw. unerwünschten Programms eine Email verschickt werden:

► Geben Sie eine Email-Adresse an.

Grundeinstellungen - Bereich Erweitert



Externes Programm Start eines externen Prozesses bei Fund verdächtiger Dateien. (Für nähere Informationen siehe [External Program](#) – Seite 37)

Log Datei Vollständiger Pfad und Dateiname der Logdatei von AntiVir Guard, z. B. /var/log/avguard.log.
Die Angaben werden zusätzlich im syslog geloggt.

► Geben Sie den vollständigen Pfad und Dateinamen ein.

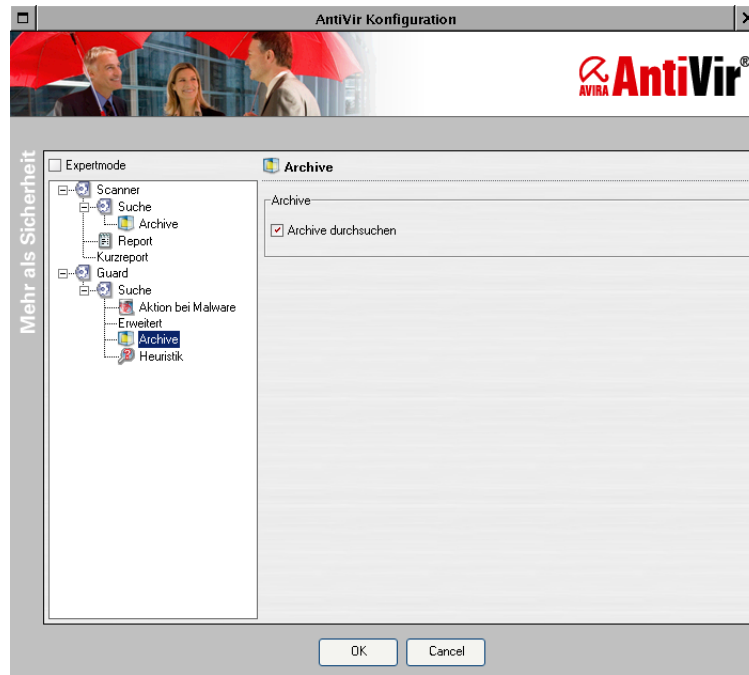
Anzahl Daemons Die Anzahl der AntiVir Guard-Dämons, die gleichzeitig laufen, kann zwischen 3 und 20 eingestellt werden. Der voreingestellte Wert 3 ist sinnvoll für kleinere Standardrechner. Für leistungsfähige Industrie-PC kann eine höhere Anzahl sinnvoll sein.

Wenn das Kontrollkästchen **AVGuard deaktivieren** gesetzt wird, wird der AntiVir Guard deaktiviert.

Hierdurch wird NumDaemons in *avguard.conf* gesetzt.

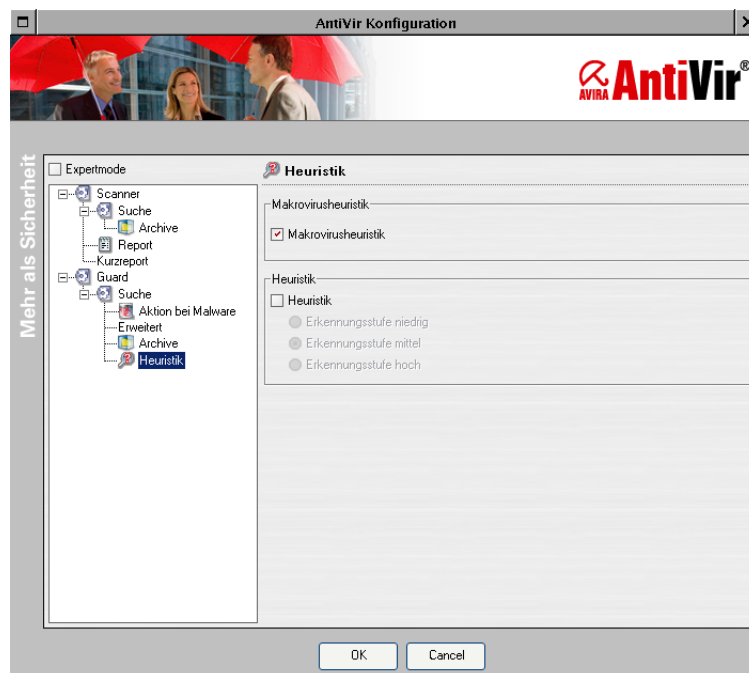
- Wählen Sie die gewünschte Anzahl der Dämons.

Grundeinstellungen - Bereich Archive



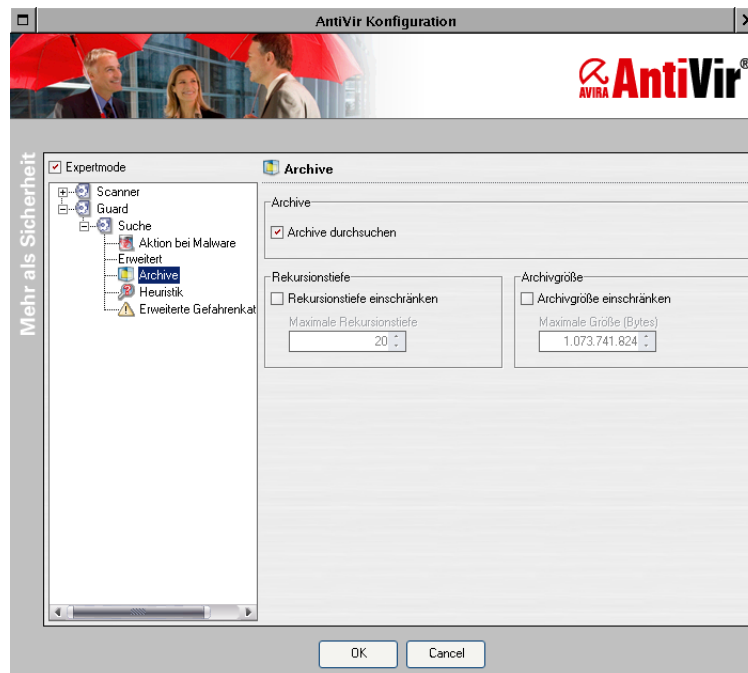
- Archive ► Wenn Archive durchsucht werden sollen:
- ↳ Aktivieren Sie das Kontrollkästchen **Archive durchsuchen**.

Grundeinstellungen - Bereich Heuristik



- Makrovirus-Heuristik ► Aktivieren Sie das Kontrollkästchen **Makrovirusheuristik** um die Heuristik für Makroviren in Dokumenten einzuschalten.
- Heuristik ► Aktivieren Sie das Kontrollkästchen **Heuristik** um die Win32-Datei-Heuristik einzuschalten, die auch unbekannte Dateiviren, Würmer, Trojaner etc. entdecken kann. Sie können einstellen, wie aggressiv die Heuristik sein soll:
- Erkennungsstufe niedrig
 - Erkennungsstufe mittel
 - Erkennungsstufe hoch

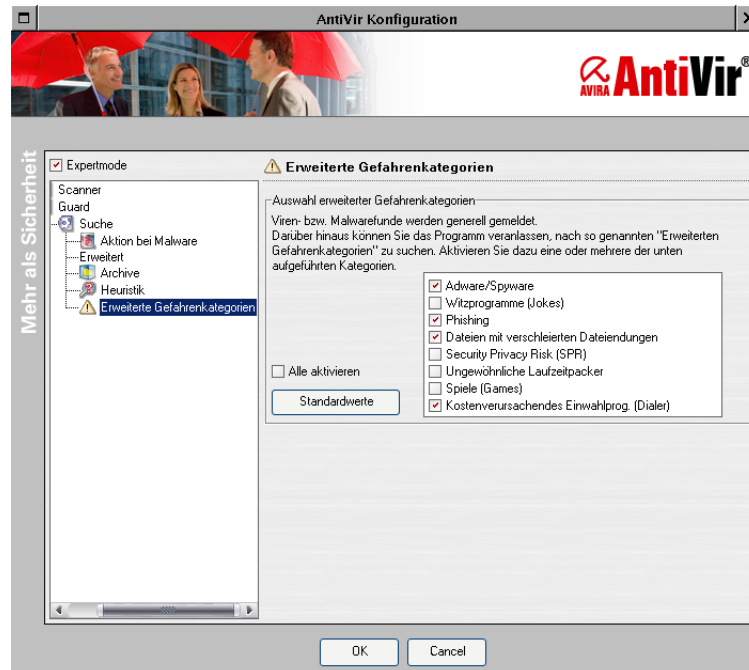
Experteneinstellungen - Bereich Archive



Im Expertenmodus haben Sie zusätzlich noch die Möglichkeit folgendes einzustellen:

- Rekursionstiefe ► Aktivieren Sie das Kontrollkästchen **Rekursionstiefe einschränken** um die Maximale Rekursionstiefe für ein Archiv festzulegen
- Archivgröße ► Aktivieren Sie das Kontrollkästchen **Archivgröße einschränken** um die Maximale Archivgröße festzulegen.

Experteneinstellungen - Erweiterte Gefahrenkategorien



Sie können AntiVir dazu veranlassen, nach so genannten **Erweiterten Gefahrenkategorien** zu suchen. Aktivieren Sie dazu eine oder mehrere der aufgeführten Kategorien.

Für eine nähere Beschreibung lesen Sie bitte den "Tooltip".

Die Liste kann sich nach einem Update ändern.

7 Service

7.1 Support

Support-Service Auf unserer Webseite <http://www.avira.de> erhalten Sie alle Informationen zu unserem umfangreichen Support-Service.

Die Kompetenz und Erfahrung unserer Entwickler stehen Ihnen hier zur Verfügung. Die Experten der Avira GmbH beantworten Ihre Fragen und helfen bei kniffligen technischen Problemen weiter.

Während der ersten 30 Tage nach Erwerb einer Lizenz haben Sie die Möglichkeit, den AntiVir Installationssupport in Anspruch zu nehmen, telefonisch, per Email oder per Online-Formular.

Darüber hinaus empfehlen wir Ihnen optional den Erwerb unseres AntiVir Classic Supports, mit dem Sie bei auftretenden technischen Problemen unsere Fachleute während der Geschäftszeiten kontaktieren und zu Rate ziehen können. Pro Jahr berechnen wir Ihnen für diesen Service, in dem auch der Virenbereinigungs- und Hoax-Support eingeschlossen sind, zwanzig Prozent des Listenpreises Ihres jeweils erworbenen AntiVir-Programms.

Der ebenfalls optional verfügbare AntiVir Premium Support bietet Ihnen über den Leistungsumfang des AntiVir Classic Supports hinaus genügend Spielraum, auch bei Notfällen außerhalb der Geschäftszeiten jederzeit einen kompetenten Ansprechpartner zu erreichen. Bei Virenalarm wird auf Wunsch eine SMS-Benachrichtigung auf Ihr Mobiltelefon gesendet.

Email-Support Support über Email erhalten Sie über <http://www.avira.de>.

7.2 Online-Shop

Sie wollen unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der Avira GmbH können Sie unter <http://www.avira.de> schnell und sicher Lizenzen erwerben, verlängern oder erweitern. Der Online-Shop führt Sie Schritt für Schritt durch das Bestell-Menü. Ein multilinguales Customer-Care-Center informiert Sie über Bestellprozesse, Zahlungsabwicklungen und Auslieferung. Wiederverkäufer können auf Rechnung bestellen und ein Reseller-Panel nutzen.

7.3 Kontakt

Postadresse Avira GmbH
Lindauer Strasse 21
D-88069 Tettnang
Deutschland

Internet Allgemeine Informationen zu uns und unseren Produkten erhalten Sie auf unserer Homepage <http://www.avira.de>.

8 Anhang

8.1 Glossar

Begriff	Erklärung
Backdoor- Steuerprogramme (BDC)	Um Daten zu stehlen oder Rechner zu manipulieren, wird ein Backdoor-Steuerprogramm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder das lokale Netzwerk kann dieses Programm über eine Backdoor-Steuersoftware (Client) von Dritten gesteuert werden.
Cron-Dämon	Dämon, der andere Programme zu vorgegebenen Zeiten startet.
Dämon	Im Hintergrund laufender Prozess zur Systemverwaltung unter UNIX. Im Schnitt laufen einige Dutzend Dämonen auf dem Rechner. Diese Prozesse werden beim Hochfahren des Rechners gestartet.
Demoversion	Ohne Lizenzdatei läuft AntiVir UNIX Server ausschließlich als Demoversion. In der Demoversion wird ein Virenfund über <i>syslog</i> gemeldet. Der Zugriff auf die betroffene Datei wird aber nicht blockiert. Alle Operationen wie Umbenennen, Reparieren oder Verschieben der betroffenen Dateien sind nicht möglich. Die Update-Funktion ist eingeschränkt.
Dialer	Kostenverursachende Einwahlprogramme. Auf dem Rechner installiert, bauen diese Programme eine Internetverbindung über eine Premium-Rate-Nummer auf, deren Tarifgestaltung ein breites Spektrum umfassen kann (Vorwahl 0900 in Deutschland, 09x0 in Österreich und in der Schweiz und mittelfristig auch in Deutschland). Manchmal werden Dialer bewusst unauffällig eingesetzt, bisweilen in betrügerischer Absicht. Dies kann zu horrenden Telefonrechnungen führen. AntiVir erkennt Dialer.
Engine	Modul der AntiVir-Software, das die Virensuche steuert.
Heuristik	Systematisches Verfahren, das mit generellen und speziellen Regeln bestimmte Probleme zu lösen versucht. Das Auffinden einer Lösung kann damit allerdings nicht garantiert werden. AntiVir verwendet ein heuristisches Verfahren zum Auffinden von noch unbekannten Makroviren. Hierbei wird das Makro beim Auffinden von virustypischen Funktionen als "verdächtig" gemeldet.
Kernel	Innerster Teil des Betriebssystems mit elementaren Systemfunktionen (Speicherverwaltung, Prozessverwaltung).
Logdatei	Auch: Reportdatei, Protokolldatei. Datei, in die Meldungen von Programmen geschrieben werden.
Malware	Oberbegriff für Software-"Fremdkörper" jeglicher Art. Dies können Störungen wie Computerviren sein, aber auch andere Software, die vom Nutzer generell als unerwünscht betrachtet wird (siehe auch Unerwünschte Programme).

Begriff	Erklärung
PMS (Possibly Malicious Software)	"Möglicherweise schädliche Software": PMS richtet normalerweise keinen Schaden auf dem eigenen Rechner an. Sie wurde programmiert, um anderen Anwendern Schaden zuzufügen. Beispiel Mailbomber: Mit einem solchen Programm kann ein Opfer mit Tausenden von Emails attackiert werden. AntiVir erkennt PMS.
Quarantäneverzeichnis	Verzeichnis, in das betroffene Dateien geschoben werden, um sie dem Zugriff der Benutzer zu entziehen.
root	Benutzer mit uneingeschränkten Rechten für die Systemverwaltung (entsprechend dem Administrator bei Windows).
Signatur	Kombinationen von Bytefolgen, an denen ein Virus oder ein unerwünschtes Programm erkannt werden kann.
Skript	Textdatei mit Befehlen, die von UNIX ausgeführt werden. (Entspricht etwa einer Batchdatei bei DOS).
SMP (Symmetric Multi Processing)	Linux SMP: Linux-Version für Rechner mit Parallelprozessoren.
SMTP	Simple Mail Transfer Protocol: Verfahren, auf dessen Basis Emails im Internet transportiert werden.
syslog-Dämon	Dämon, der die Meldungen diverser Programme protokolliert. Die Meldungen werden in unterschiedliche Logdateien geschrieben. Die Konfiguration des <i>syslog</i> -Dämons wird in <i>/etc/syslog.conf</i> festgelegt.
Unerwünschte Programme	Oberbegriff für Programme, die keinen direkten Schaden auf dem Rechner verursachen oder ohne Absicht des Anwenders oder Administrators installiert wurden. Hierzu zählen Backdoor-Steuerprogramme, Dialer, Witzprogramme und auch Spiele. AntiVir erkennt verschiedene Arten unerwünschter Programme.
VDF (Virus Definition File)	Virendefinitionsdatei: Datei mit den Signaturen der bekannten Viren. In vielen Fällen ist es für ein Update ausreichend, diese Datei zu aktualisieren.
VFS	Virtual File System
Virendefinitionsdatei	siehe VDF

8.2 Weitere Infoquellen

Weitere Informationen zu verschiedenen Viren, Würmern, Makroviren und weiteren unerwünschten Programmen sind erhältlich unter
<http://www.avira.de/de/threats/index.html>

8.3 Goldene Regeln zur Virenvorsorge

- ▶ Erstellen Sie Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkserver und die einzelnen Workstations. Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- ▶ Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Disketten ohne ausführbare Programme enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- ▶ Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an.
- ▶ Begrenzen Sie den Programmaustausch: Das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- ▶ Prüfen Sie neue Programme vor und nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, lässt sich ein Virus in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu Ihrem Rechner, sollten Sie folgende Spielregeln zum Schutz vor Viren beachten:

- ▶ Stellen Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerk-Medien) und von Downloads bereit. Trennen Sie diesen Rechner aber vom Netzwerk!
- ▶ Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist, und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus notwendigen Schritte.
- ▶ Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/Veränderungen aufgrund von Inkompatibilitäten vermindern helfen. Programme und Massenspeicher lassen sich ersetzen; Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- ▶ Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- ▶ Sorgen Sie für ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird. Es ist ein guter Schutz gegen Viren.

www.avira.de



Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telefon: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Email: info@avira.de
Internet: <http://www.avira.de>

© Avira GmbH. Alle Rechte vorbehalten.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira GmbH nicht gestattet.

Irrtümer und technische Änderungen vorbehalten.

Ausgabe Mai 2007

AntiVir® ist ein registriertes Warenzeichen der Avira GmbH. Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

