

Sicherheit und mehr ...



**BusinessSolutions**



## Benutzerhandbuch

### UNIX Server



---

# Inhaltsverzeichnis

<b>1</b>	<b>Über dieses Handbuch</b>	<b>3</b>
1.1	Einleitung	3
1.2	Aufbau des Handbuchs	4
1.3	Zeichen und Symbole	5
1.4	Abkürzungen	6
<b>2</b>	<b>Produktinformationen</b>	<b>7</b>
2.1	Leistungsumfang	8
2.2	Lizenzierungskonzept	9
2.3	Funktionsweise von AntiVir	11
2.4	Systemvoraussetzungen	12
2.5	Technische Informationen	12
<b>3</b>	<b>Installation</b>	<b>13</b>
3.1	Installationsdateien bereitstellen	13
3.2	Lizenzierung	14
3.3	Erstellen des Kernel-Moduls Dazuko	15
3.4	Anbindung an Samba	17
3.5	AntiVir installieren	20
3.6	AntiVir erneut installieren	28
3.7	AntiVir UNIX Server über grafische Installationsroutine installieren	29
3.8	Anbindung an Produkte von Fremdherstellern	36
<b>4</b>	<b>Konfiguration</b>	<b>37</b>
4.1	Übersicht	38
4.2	Konfigurationsdateien	38
4.3	Konfigurationsskripte	47
4.4	Konfigurieren der Nachrichten von AntiVir	50
4.5	Konfigurieren des residenten Wächters AntiVir Guard	53
4.6	Konfigurieren des AntiVir Samba Scanners	63
4.7	Konfigurieren regelmäßiger Updates	67
4.8	AntiVir UNIX Server testen	74
<b>5</b>	<b>Bedienung</b>	<b>75</b>
5.1	AntiVir Kommandozeilenscanner im Überblick	75
5.2	AntiVir Kommandozeilenscanner in der Anwendung	81
5.3	Vorgehen bei Fund eines Virus/unerwünschten Programms	86

---

<b>6</b>	<b>Grafische Benutzeroberfläche (GUI)</b> .....	87
6.1	Übersicht .....	87
6.2	AntiVir Scanner .....	89
6.2.1	AntiVir Scanner über GUI bedienen.....	89
6.2.2	AntiVir Scanner über GUI konfigurieren.....	94
6.3	AntiVir Guard .....	100
6.3.1	AntiVir Guard über GUI bedienen.....	100
6.3.2	AntiVir Guard über GUI konfigurieren.....	104
<b>7</b>	<b>Service</b> .....	109
7.1	Support .....	109
7.2	Online-Shop .....	109
7.3	Kontakt .....	110
<b>8</b>	<b>Anhang</b> .....	111
8.1	Glossar .....	111
8.2	Weitere Infoquellen .....	113
8.3	Goldene Regeln zur Virenvorsorge .....	114

# 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 4
- [Zeichen und Symbole](#) – Seite 5

## 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 109).

Ihr Team von AntiVir


### 1.2 Aufbau des Handbuchs

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

Kapitel	Inhalt
<a href="#">1 Über dieses Handbuch</a>	Aufbau des Handbuchs, Zeichen und Symbole
<a href="#">2 Produktinformationen</a>	Allgemeine Hinweise zur Software AntiVir, zu Aufbau, Funktionsweise, Systemvoraussetzungen und Lizenzierung
<a href="#">3 Installation</a>	Anleitung zur Installation von AntiVir UNIX Server auf Ihrem System – sowohl Skript-basiert als auch über eine grafische Installationsroutine
<a href="#">4 Konfiguration</a>	Anleitung zur optimalen Anpassung von AntiVir auf Ihr System
<a href="#">5 Bedienung</a>	Die Arbeit mit AntiVir, nachdem es installiert wurde; gezielte Suche nach Viren und unerwünschten Programmen; Verhalten beim Auffinden von Viren und unerwünschten Programmen
<a href="#">6 Grafische Benutzeroberfläche (GUI)</a>	Allgemeine Hinweise zur GUI; Bedienung und Konfiguration von AntiVir UNIX Server über die GUI
<a href="#">7 Service</a>	Support und Service von H+BEDV
<a href="#">8 Anhang</a>	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
i	... 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
<code>Strg</code> + <code>Alt</code>	Taste bzw. Tastenkombination
<code>/usr/lib/AntiVir/antivir</code>	Dateinamen und Pfadangaben
<code>ls usr/lib/AntiVir</code>	Eingaben des Anwenders
<b>Komponente auswählen</b> <b>Alles Markieren</b>	Elemente der Software-Oberfläche wie Menüpunkte, Fenstertitel, Schaltflächen in Dialogfenstern
<a href="http://www.antivir.de">http://www.antivir.de</a>	URLs
Zeichen und Symbole – Seite ...	Querverweise innerhalb des Dokuments

### 1.4 Abkürzungen

In diesem Handbuch werden folgende Abkürzungen verwendet:

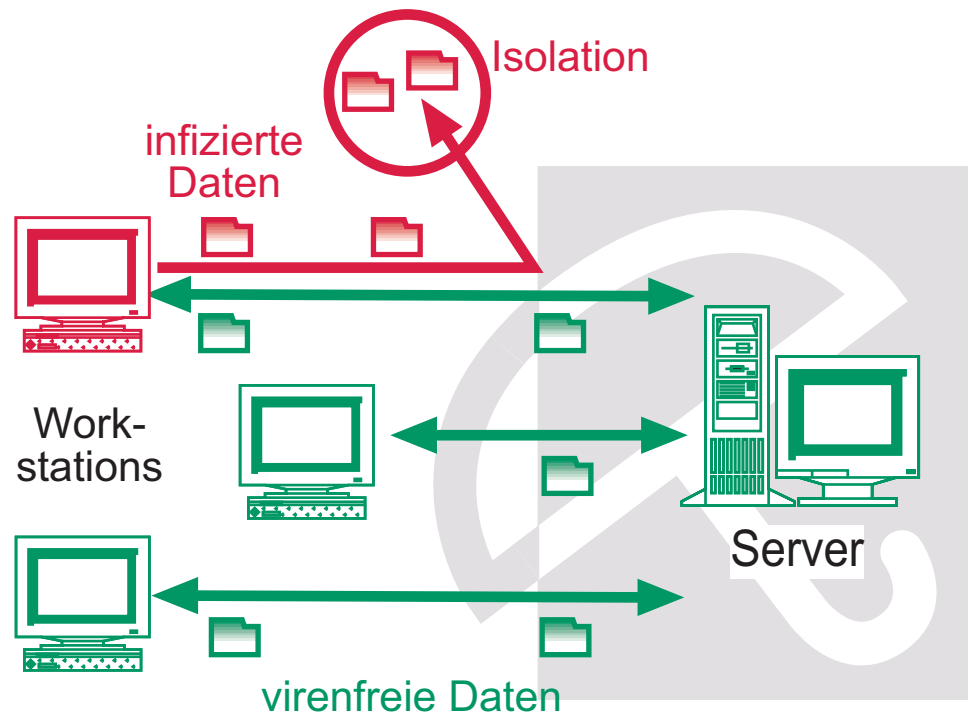
<b>Abkürzung</b>	<b>Erläuterung</b>
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
GPL	General Public License
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
PMS	Possible Malicious Software
RFC	Request For Comment
SMTP	Simple Mail Transfer 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 Konfigurationsskripte 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, Sperren, 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.antivir.de/dateien/antivir/handbuch/pdf/eula\\_antivir.pdf](http://www.antivir.de/dateien/antivir/handbuch/pdf/eula_antivir.pdf)).

Sie können die vielfältigen Funktionen von AntiVir MailGate 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 avmgate.key vergeben. Diese erhalten Sie von H+BEDV Datentechnik 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 H+BEDV Datentechnik GmbH enthalten.

**Demoversion** Ohne Lizenzdatei läuft AntiVir MailGate als Demoversion. Dabei wird in jede Email ein Werbebanner von H+BEDV eingefügt. Ein automatisches Update ist nicht möglich, d. h. neue Virendefinitionsdateien und eine neue AntiVir Search Engine müssen immer manuell von der Webseite heruntergeladen werden.

Es besteht keine Möglichkeit, den Zugriff auf betroffene Dateien zu sperren oder sie über AntiVir zu reparieren oder zu verschieben.

**Evaluation Version** Nähere Informationen zur Evaluation Version erhalten Sie auf unserer Webseite <http://www.antivir.de>.

**Vollversion** Zum Leistungsumfang einer Vollversion gehören:

- 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    Das Komfortpaket enthält zusätzlich zur lizenzierten Vollversion:
- Alle drei Monate: Kostenlose Lieferung einer bootfähigen CD-ROM mit dem AntiVir Rescue-System und allen aktuellen AntiVir-Programmen
  - Umfangreiches Installationshandbuch (gedruckt) bei der Erstauslieferung
  - Lizenzdatei auf Diskette bei der Erstauslieferung
  - 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 ab i386
- 8 MB freier Speicherplatz auf der Festplatte
- 10 MB temporärer Speicherplatz auf der Festplatte
- 32 MB freier Hauptspeicher (empfohlen: 64 MB)
- Linux mit GLIBC oder LIBC5 bzw. FreeBSD, OpenBSD oder Sun Sparc Solaris
- bei Einsatz des Samba Scanners: Samba-Version mit Unterstützung für den VFS-Mechanismus (ab Version 2.2.0)

Wenn Sie die GUI verwenden wollen:

- Zusätzlich 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 13
- [Lizenzierung](#) – Seite 14
- [Erstellen des Kernel-Moduls Dazuko](#) – Seite 15
- [Anbindung an Samba](#) – Seite 17
- [AntiVir installieren](#) – Seite 20
- [AntiVir erneut installieren](#) – Seite 28
- [AntiVir UNIX Server über grafische Installationsroutine installieren](#) – Seite 29
- [Anbindung an Produkte von Fremdherstellern](#) – Seite 36

### 3.1 Installationsdateien bereitstellen

#### Programmdatei aus dem Internet laden

- ▶ Laden Sie die aktuelle Datei von unserer Webseite <http://www.antivir.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>/src`
- ▶ 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 9). 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@antivir.de](mailto:info@antivir.de)), um eine gültigen 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.antivir.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 21.

---

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*'
```

---

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 sollten Sie dennoch die Installation fortführen. Schlimmstenfalls gelingt später die Integration von Dazuko in Ihren UNIX-Kernel nicht. Das AntiVir-Installationsskript prüft dies aber und gibt gegebenenfalls eine Meldung aus.

---

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

```
cd /tmp/antivir-server-prof-<version>/src/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 eine Datei `dazuko.o` im temporären Verzeichnis `/tmp/antivir-server-prof-<version>/src/dazuko-<version>`.

Diese Datei wird später vom AntiVir-Installationsskript benötigt.

---



Weitere aktuelle Information zu Dazuko erhalten Sie auf der Webseite <http://www.dazuko.org>.

---

## 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 63). Neben Samba muss kein zusätzlicher 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 Internet Updater 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 20
- Wenn Dazuko noch nicht kompiliert wurde: [AntiVir ohne den AntiVir Guard installieren](#) – Seite 21
- Wenn Dazuko bereits kompiliert wurde: [AntiVir mit dem AntiVir Guard installieren](#) – Seite 24

#### 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
```

- ↳ Das Installationsskript läuft an. Zunächst werden die Programmdateien kopiert:

```
1) installing command line scanner
creating install directory /usr/lib/AntiVir ... done
checking for existing /etc/antivir.conf ... not found
copying bin/antivir to /usr/lib/AntiVir ... done
copying vdf/antivir.vdf to /usr/lib/AntiVir ... done
copying conf/antivir.conf to /etc ... done
copying sh/configantivir to /usr/lib/AntiVir ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antvir
... done
installation of command line scanner complete
```

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

```
2) installing automatic internet updater
...
Would you like to install the automatic internet
updater? [n]
```



Der Internet Updater 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 83  
Für die Erstinstallation wird aber eine Installation des Internet Updater empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren.

Installation  
mit Updater

Wenn Sie den Internet Updater installieren wollen (empfohlen):

- Geben Sie **Y** ein und bestätigen Sie mit **[Enter]**.

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

```
copying sh/avupdater to /usr/lib/AntiVir ... done

Would you like the automatic updater to start
automatically? [y]
```

- Bestätigen Sie **[Enter]**. Sie können diese Einstellung später wieder rückgängig machen.

↳ Der automatische Systemstart wird konfiguriert:

```
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avupdater to /
usr/lib/AntiVir/avupdater ...
runlevel 0 ... done
runlevel 1 ... done
runlevel 2 ... done
runlevel 3 ... done
runlevel 4 ... done
runlevel 5 ... done
runlevel 6 ... done
installation of automatic internet updater complete
```

Installation  
ohne Updater

Wenn Sie den Internet Updater später oder gar nicht installieren wollen:

- Geben Sie **N** ein oder drücken Sie **[Enter]**.
- Bestätigen Sie mit **[Enter]**.

AntiVir  
Guard  
abwählen

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

```
3) installing AvGuard
Version 2.1.3 of AntiVir for UNIX is capable of on-
access, real-time scanning of files.
...
There are several ways in which you can install
AvGuard.

module - Dazuko will be loaded by the avguard script
kernel - Dazuko is always loaded (an 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? [n]
```

- 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
...
Would you like to install the GUI? [n]
```



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      Am Schluss haben Sie die Möglichkeit, AntiVir zu konfigurieren:

```
5) configuring AntiVir
Would you like to configure AntiVir now? [y]
```



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.
  - ↳ Zum Schluss erhalten Sie die Bestätigung, dass die Installation erfolgreich verlaufen ist:

```
Installation of the following features complete:
  AntiVir command line scanner
  AntiVir Automatic Internet Updater
```

### AntiVir mit dem AntiVir Guard installieren

- ✓ Stellen Sie sicher, dass das Kernel-Modul Dazuko bereits kompiliert ist (siehe [Erstellen des Kernel-Moduls Dazuko](#) – Seite 15).

- Geben Sie ein:

```
./install
```

- ↳ Das Installationsskript läuft an. Zunächst werden die Programmdateien kopiert:

```
1) installing command line scanner
creating install directory /usr/lib/AntiVir ... done
checking for existing /etc/antivir.conf ... not found
copying bin/antivir to /usr/lib/AntiVir ... done
copying vdf/antivir.vdf to /usr/lib/AntiVir ... done
copying conf/antivir.conf to /etc ... done
copying sh/configantivir to /usr/lib/AntiVir ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir
... done
installation of command line scanner complete
```

Anschließend wird gefragt, ob der Internet Updater installiert werden soll:

```
2) installing automatic internet updater
...
Would you like to install the automatic internet
updater? [n]
```



Der Internet Updater 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 83. Für die Erstinstallation wird aber eine Installation des Internet Updater empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren.

---

Installation  
mit Updater

Wenn Sie den Internet Updater installieren wollen (empfohlen):

- Geben Sie **Y** ein und drücken Sie **[Enter]**.

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

```
copying sh/avupdater to /usr/lib/AntiVir ... done
```

```
Would you like the automatic updater to start automatically? [y]
```

- Bestätigen Sie diese Frage mit **Y** oder **[Enter]**. Sie können diese Einstellung später wieder rückgängig machen.

↳ Der automatische Systemstart wird konfiguriert:

```
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avupdater to /usr/lib/AntiVir/avupdater ...
```

```
runlevel 0 ... done
```

```
runlevel 1 ... done
```

```
runlevel 2 ... done
```

```
runlevel 3 ... done
```

```
runlevel 4 ... done
```

```
runlevel 5 ... done
```

```
runlevel 6 ... done
```

```
installation of automatic internet updater complete
```

Installation  
ohne Updater

Wenn Sie den Internet Updater später oder gar nicht installieren wollen:

- Geben Sie **N** ein und drücken Sie **[Enter]**.

AntiVir  
Guard  
installieren

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

```
3) installing AvGuard
```

```
Version 2.0.7 of AntiVir for UNIX is capable of on-access, real-time scanning of files.
```

```
...
```

```
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 avguard script)
```

```
no install - do not install AvGuard at this time
```

```
...
```

```
available options: m k n
```

```
How should AvGuard be installed? [n]
```

- Geben Sie **M** ein und bestätigen Sie mit **[Enter]**.

- ↳ Sie werden nach dem Pfad zum kompilierten Dazuko-Modul `dazuko.o` gefragt:

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

- Geben Sie den vollständigen Pfad zu `dazuko.o` ein.

**Beispiel:** Wenn `dazuko.o` in `/tmp/antivir-server-prof-<version>/src/dazuko-<version>/` liegt, geben Sie ein:

```
/tmp/antivir-server-prof-<version>/src/dazuko-<version>/dazuko.o
```

- ↳ Das Installationsskript testet, ob `dazuko.o` korrekt kompiliert wurde, und kopiert anschließend die Dateien für den AntiVir Guard.

```
testing /tmp/antivir-<version>-server/src/dazuko-
<version>/dazuko.o ... ok
detecting kernel version ... linux-2.4.18-4GB
copying /tmp/dazuko.o to /usr/lib/AntiVir/linux-
2.4.18-4GB ... done
copying sh/avguard to /usr/lib/AntiVir ... done
linking configavguard to configantivir ... 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.

```
identifying startup script location ... found (etc/
rc.d/)
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avguard to /usr/
lib/AntiVir/avguard ...
runlevel 0 ... done
runlevel 1 ... done
runlevel 2 ... done
runlevel 3 ... done
runlevel 4 ... done
runlevel 5 ... done
runlevel 6 ... done
installation of AvGuard complete
```

GUI  
installieren

Anschließend wird gefragt, ob AntiVir mit der optionalen grafischen Be-

nutzeroberfläche (GUI) installiert werden soll:

```
4) installing GUI
...
Would you like to install the GUI? [n]
```



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.

Konfigura-  
tion starten

Am Schluss haben Sie die Möglichkeit, AntiVir zu konfigurieren:

```
5) configuring AntiVir
Would you like to configure AntiVir now? [y]
```



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.
  - ↳ Zum Schluss erhalten Sie die Bestätigung, dass die Installation erfolgreich verlaufen ist:

```
Installation of the following features complete:
  AntiVir command line scanner
  AntiVir Automatic Internet Updater
  AntiVir Guard
```

### 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 37), werden dabei nicht überschrieben, sondern übernommen.
- Nachinstallation einzelner Komponenten, z. B. des AntiVir Guard oder des Internet Updater.
- Aktivierung oder Deaktivierung des automatischen Starts des Internet Updater 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 20).

- ▶ 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 13 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.



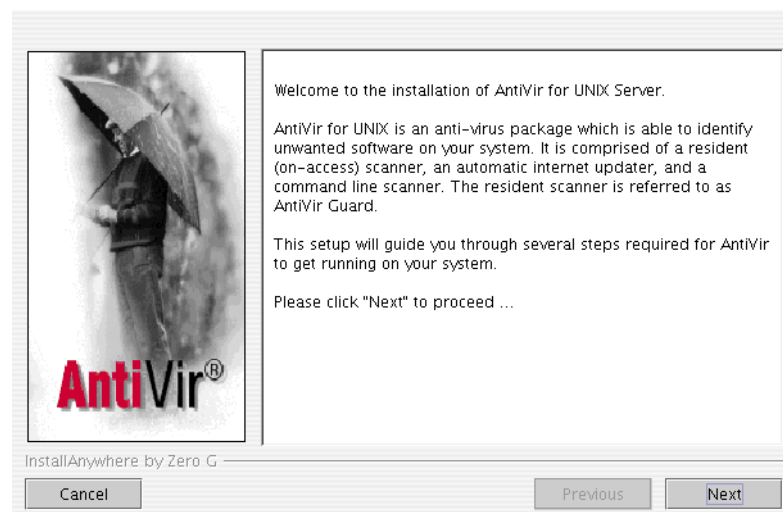
AntiVir UNIX Server mit grafischer Installationsroutine ist nur für Linux verfügbar. Es wird Java 1.4.0 oder höher benötigt.

✓ Die Programmdatei wurde entpackt und liegt im Verzeichnis `/tmp/antivir-server-linux-gui_installer`.

► Geben Sie ein:

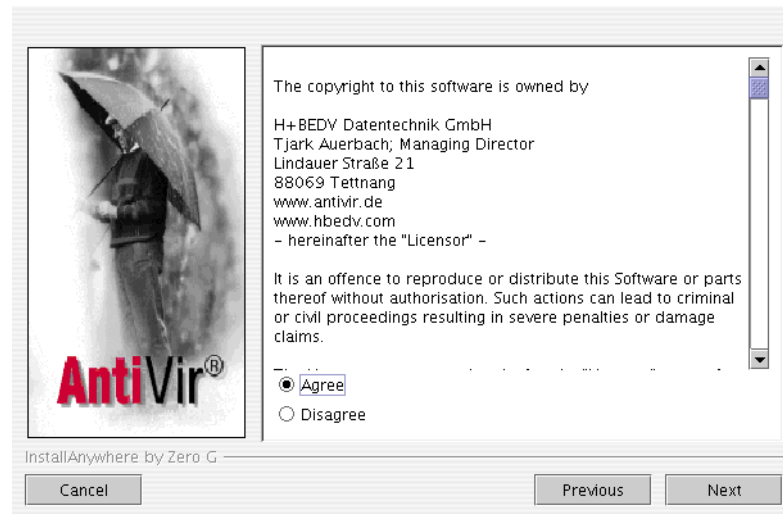
```
./install
```

↳ Es erscheint der Begrüßungstext und eine kurze Beschreibung des Programms:



► Klicken Sie auf **Next**.

↳ Das folgende Dialogfenster mit den Lizenzbedingungen erscheint:

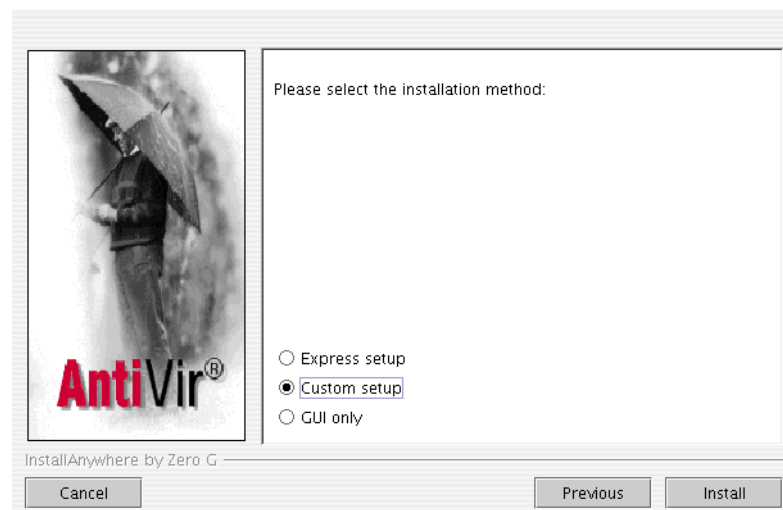


**i**

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:

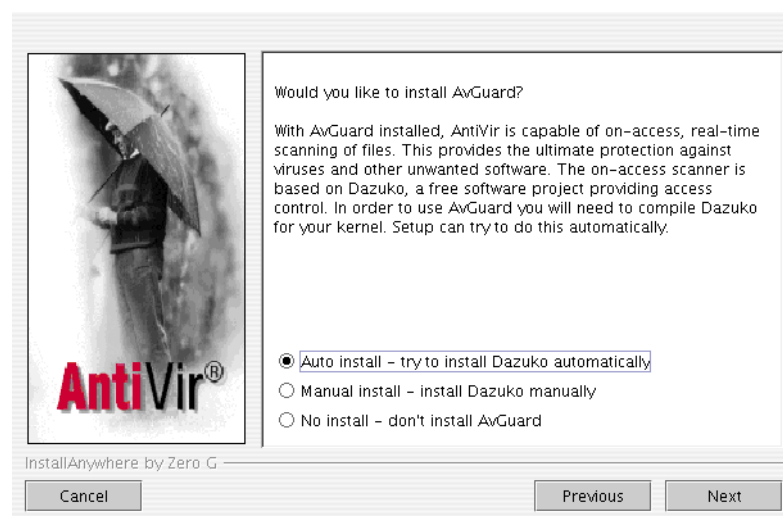
`/usr/lib/AntiVir`

- Es wird der AntiVir Guard (on-access scanner) installiert.
  - Es wird kein automatischer Internet Updater 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

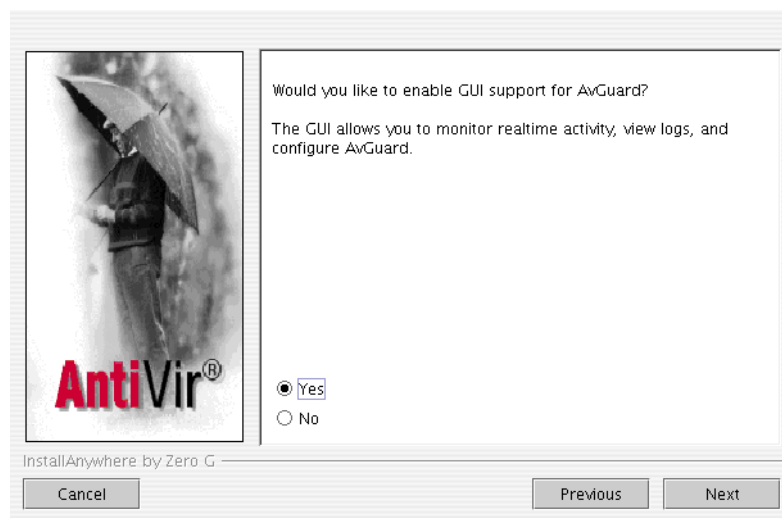
Sie können das Programm auch mit benutzerdefinierten Einstellungen installieren.

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

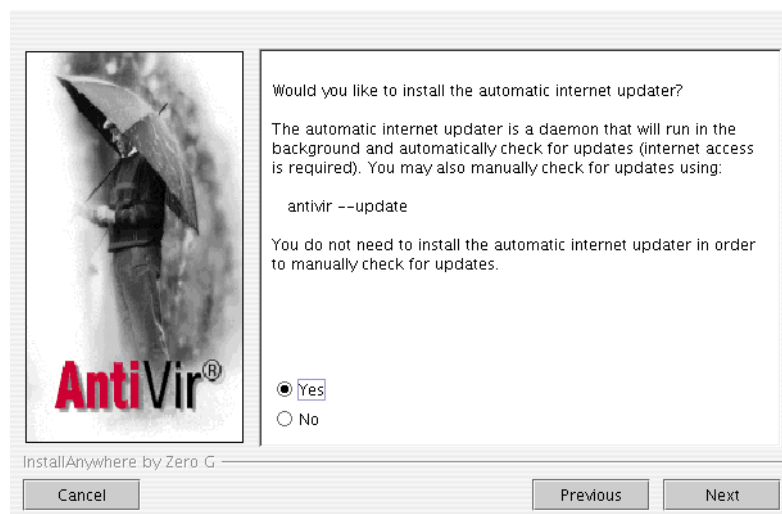


Sie haben drei Möglichkeiten, den AntiVir Guard zu installieren:

- **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 15)
  - **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`):

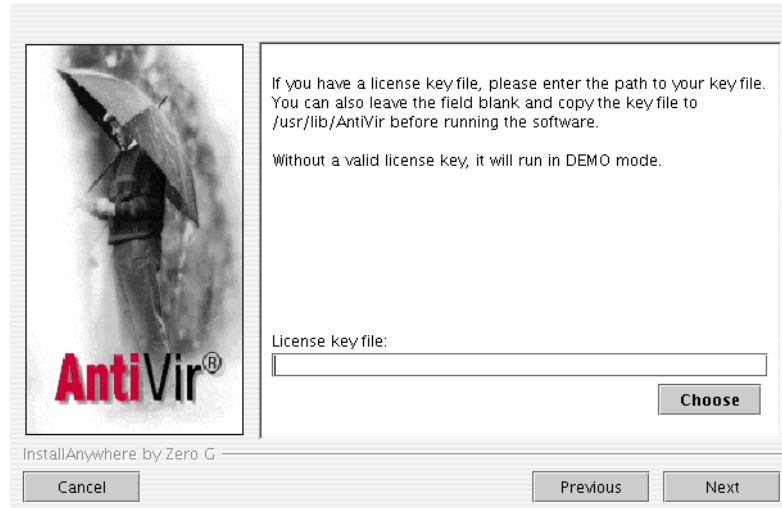


- Aktivieren Sie **Yes** oder **No** und klicken Sie auf **Next**.
- ↳ Im folgenden Dialogfenster wird abgefragt, ob der automatische Internet Updater installiert werden soll:

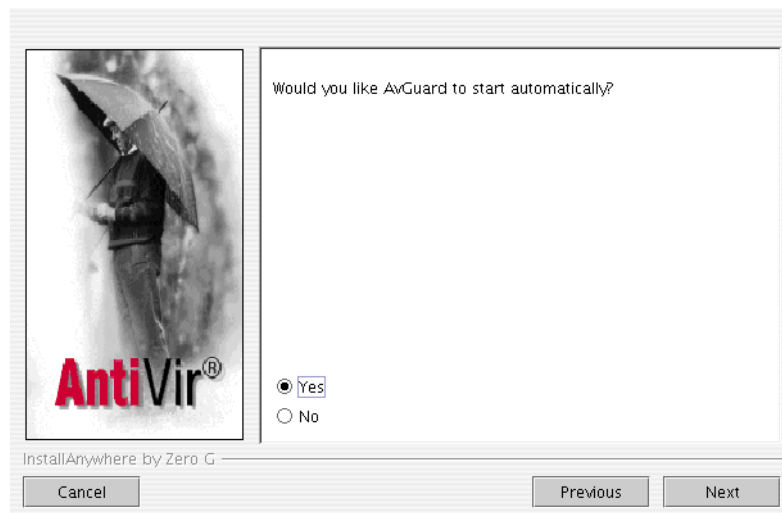


Wenn der Internet Updater installiert werden soll:

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

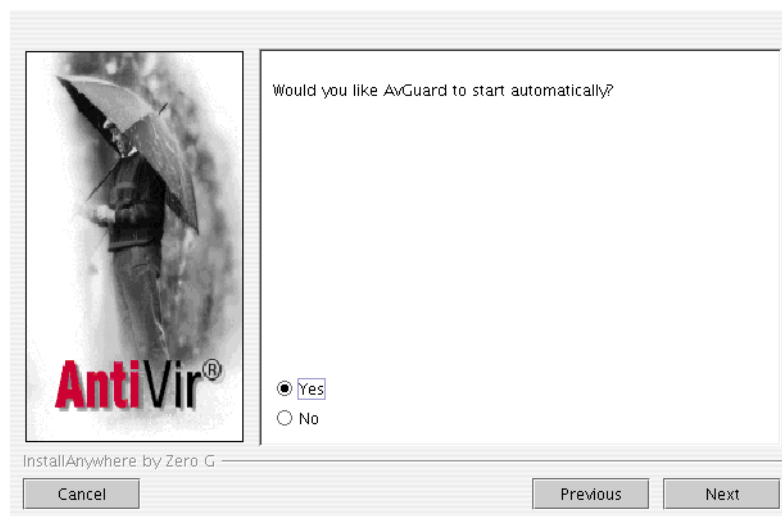


- ▶ Folgen Sie den Anweisungen und klicken Sie auf **Next**.
  - ↳ Im folgenden Dialogfenster wird abgefragt, ob der AntiVir Guard beim Booten des Rechners automatisch gestartet werden soll:



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

- ↳ Optional wird im folgenden Dialogfenster abgefragt, ob der Internet Updater 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

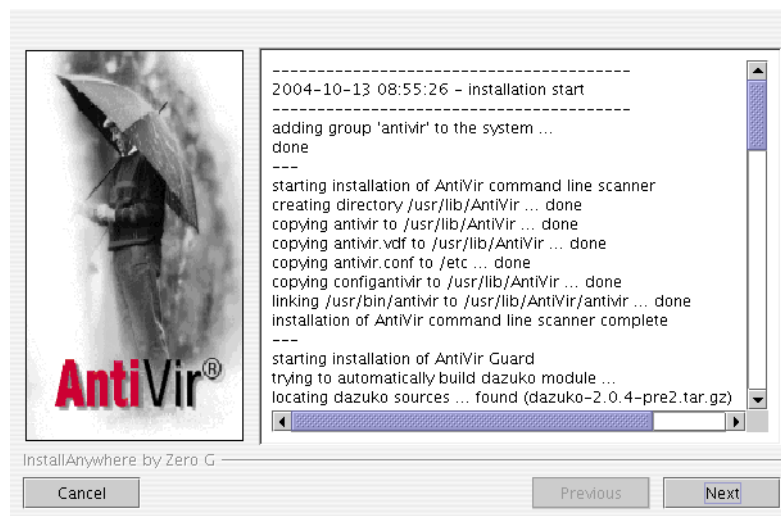
Wählen Sie diese Installationsart, wenn Sie nur die GUI installieren wollen.

- ▶ Aktivieren Sie **GUI only** und klicken Sie auf **Next**.
  - ↳ Die GUI wird im folgenden Verzeichnis installiert:  
`/usr/lib/AntiVir`

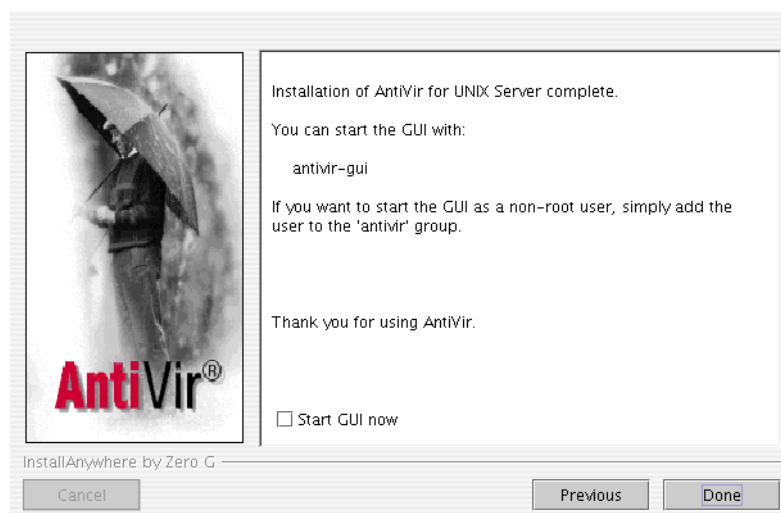
- ↳ Ein Dialogfenster erscheint, indem alle Einstellungen und weitere Anweisungen angezeigt werden:
- Klicken Sie auf **Install**.
- ↳ Die GUI wird installiert.

## 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 38. Wenn Sie die Konfigurationsskripte verwenden möchten, können Sie diesen Abschnitt überschlagen.
- Erklärungen zum allgemeinen Umgang mit den Konfigurationsskripten erhalten Sie in [Konfigurationsskripte](#) – Seite 47
- Spezifische Konfigurationen von AntiVir werden erläutert in
  - [Konfigurieren der Nachrichten von AntiVir](#) – Seite 50
  - [Konfigurieren des residenten Wächters AntiVir Guard](#) – Seite 53
  - [Konfigurieren des AntiVir Samba Scanners](#) – Seite 63
  - [Konfigurieren regelmäßiger Updates](#) – Seite 67
- Abschließend wird in [AntiVir UNIX Server testen](#) – Seite 74 erklärt, wie Sie die korrekte Konfiguration von AntiVir prüfen.

### 4.1 Übersicht

Konfigurationsdateien

Die Konfiguration wird in drei Dateien definiert:

- `antivir.conf` definiert das automatische Update der Software und die Protokollierung beim Auftreten von Viren und unerwünschten Programmen.
- `avguard.conf` definiert das Verhalten des residenten Wächters AntiVir Guard.
- `vscan-antivir.conf` definiert das Verhalten des AntiVir Samba Scanners; diese Datei wird in Kapitel [4.6 Konfigurieren des AntiVir Samba Scanners](#) detailliert beschrieben.



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

Komfortabler ist aber die Einstellung über die Konfigurationsskripte, die im Programmpaket enthalten sind. Diese Skripte fangen eventuelle Fehleingaben ab und starten die notwendigen Prozesse neu.

---

Konfigurationsskripte

Zwei Konfigurationsskripte stehen in `/usr/lib/AntiVir` zur Verfügung:

- `configantivir` editiert die Einstellungen in `antivir.conf`.
- `configavguard` editiert die Einstellungen in `avguard.conf` und anschließend in `antivir.conf`, da sich diese ebenfalls auf den AntiVir Guard auswirken.

### 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 die Konfigurationsskripte verwenden, müssen Sie anschließend den Internet Updater 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 104.

Num  
Daemons

### Anzahl Dämonen:

Die Anzahl der AntiVir Guard-Dämonen, die gleichzeitig laufen, kann zwischen 0 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
```

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
```

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 (siehe [Ausgeschlossene Verzeichnisse definieren](#) – Seite 54). 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

## Überwachte Archive:

Der AntiVir Guard scannt zusätzlich komprimierte Archive beim Zugriff, abhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`. Hierfür muss folgende Option aktiviert werden:

```
ArchiveScan
```

In der Voreinstellung ist diese Option deaktiviert, um die Performance von AntiVir möglichst hoch zu halten.

ArchiveMax  
Size

## Maximale Archivgröße:

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):

```
ArchiveMaxSize      1073741824
```

ArchiveMax  
Recursion

## Rekursionstiefe für Archive:

Wenn rekursiv gepackte Archive gescannt werden, kann die Rekursionstiefe auf `ArchiveMaxRecursion` beschränkt werden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

```
ArchiveMaxRecursion 5
```

Archive  
MaxRatio

## Dekompressionsfaktor für Archive:

Mit diesem Eintrag wird der Scanvorgang auf Dateien beschränkt, die einen vorgegebenen Dekompressionsfaktor nicht überschreiten. Diese Maßnahme schützt vor so genannten "Mailbomben", die beim Dekomprieren unerwartet viel Speicherplatz belegen würden. Bei einem Wert von 0 findet keine Beschränkung statt. Voreingestellt:

```
ArchiveMaxRatio      150
```



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:

<b>Option</b>	<b>Funktion</b>
%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
%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)



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.

### Konfigurationsdatei antivir.conf

Im Folgenden werden die Einträge in antivir.conf kurz beschrieben. Diese Einträge beeinflussen alle AntiVir-Programme, die auf dem Rechner installiert sind. Daher wird in diesem Abschnitt auch allgemein von "AntiVir" und nicht von "AntiVir UNIX Server" gesprochen.

Wie Sie diese Datei komfortabel über ein Skript editieren können, erfahren Sie in [Konfigurationsskripte](#) – Seite 47.



Wenn Sie manuell Werte in antivir.conf ändern, die den Internet Updater betreffen, und nicht das Konfigurationsskript verwenden, müssen Sie anschließend den Internet Updater manuell neu starten. Erst dann werden die Änderungen wirksam.

► Geben Sie dafür ein:

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

---

EmailTo **Email-Nachrichten:**

AntiVir kann Emails verschicken, wenn ein Virus oder unerwünschtes Programm entdeckt wird. Eine Voreinstellung gibt es nicht. Damit Emails verschickt werden können, muss also ein Adressat angegeben werden, z. B:

```
EmailTo root@localhost
```

LogTo **Logdatei:**

Alle wichtigen Operationen von AntiVir werden über den syslog-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:

```
LogTo /var/log/antivir.log
```

AutoUpdate... **Update-Plan:**

Die Software kann mit Hilfe des Internet Updater regelmäßig online auf Updates geprüft und, wenn nötig, aktualisiert werden. Als Voreinstellung sind die möglichen Optionen aus Sicherheitsgründen deaktiviert, es wird also kein automatisches Update durchgeführt.

Für Updates alle 2 Stunden muss folgende Option aktiviert werden:

```
AutoUpdateEvery2Hours
```

Für tägliche Updates muss folgende Option aktiviert werden:

```
AutoUpdateDaily
```

Wenn tägliche Updates eingestellt sind, kann in einem weiteren Eintrag die Uhrzeit für die Updates als HH:MM angegeben werden, z. B.:

```
AutoUpdateTime 04:23
```

HTTPProxy...

## Proxyserver:

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:

- HTTP-Proxyserver
- Port
- Username und Passwort, wenn diese für den HTTP-Proxyserver erforderlich sind.

Beispiel:

```
HTTPProxyServer    proxy.domain.com
HTTPProxyPort      8080
HTTPProxyUsername  username
HTTPProxyPassword  password
```

Updater  
Keeps  
Backups

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.

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.

Syslog...

## Syslog-Einstellung:

Für alle wichtigen Operationen gibt AntiVir Meldungen an den syslog-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:

```
SyslogFacility    user
SyslogPriority     notice
```

Diese Werte gelten auch, wenn die Einträge deaktiviert sind.

GnuPG... **GnuPG-Einstellung:**

Die Authentizität der AntiVir-Updates kann durch GnuPG sichergestellt werden. Nähere Informationen hierzu siehe Abschnitt [Authentizität der Updates durch GnuPG sicherstellen](#) – Seite 72. 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.

Detect... **Erkennung weiterer unerwünschter Programme:**

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:

```
DetectDialer
```

```
DetectJoke
```

```
DetectGame
```

```
DetectPMS
```

Heuristics **Makroviren-Heuristik:**

Macro

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

```
HeuristicsMacro
```

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
```



## 4.3 Konfigurationsskripte

Mit Hilfe der Konfigurationsskripte kann AntiVir komfortabel angepasst werden. Diese Skripte fangen eventuelle Fehleingaben ab und starten die notwendigen Prozesse neu.

Es gibt zwei Konfigurationsskripte bei AntiVir:

- configantivir editiert die Einstellungen in antivir.conf
- configavguard editiert die Einstellungen in avguard.conf und anschließend in antivir.conf, da sich diese ebenfalls auf den AntiVir Guard auswirken.

Der Umgang mit den Skripten ist sehr einfach.

Wenn Sie AntiVir allgemein konfigurieren wollen:

- Geben Sie ein:

```
/usr/lib/AntiVir/configantivir
```

Wenn Sie den AntiVir Guard konfigurieren wollen:

- Geben Sie ein:

```
/usr/lib/AntiVir/configavguard
```

Die Skripte lesen die aktuell gesetzten Werte in antivir.conf bzw. avguard.conf ein und fragen systematisch, ob neue Werte gesetzt werden sollen. Die möglichen neuen Werte werden angezeigt, die alten Werte werden dabei als Default vorgeschlagen.

Wenn Sie einen vorhandenen Wert übernehmen wollen:

- Drücken Sie .

Wenn Sie einen Wert ändern wollen:

- Geben Sie den neuen Wert ein.

Am Schluss wird eine Zusammenfassung der Konfiguration angezeigt.

Nach dem Ablauf von configavguard erscheint etwa folgende Ausgabe:

```
Here are the configuration settings you have speci-
fied. Look them over to make sure they are correct.
number of daemons:                3
scan on:                          open/close
repair concerning files:          yes
handling of concerning files:     move to /tmp/unwanted
include paths:                    /usr/lib:/usr/bin:/home
exclude paths:                    /home/myhome
scan archives:                    yes
max archive size:                 1073741824 bytes
max archive recursion:            5 levels
max archive ratio                  150:1
email notification:               root@localhost
specific logfile:                 /var/log/antivir.log
update frequency:                 daily (if avupdater is
                                   running)
update time:                      random (if avupdater is
                                   running)
http proxy server:                proxy.domain.com:8080
syslog output:                    user.notice
available options:                y n
Save configuration settings? [y]
```

Wenn nicht alle Angaben der gewünschten Konfiguration entsprechen:

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

Wenn alle Angaben der gewünschten Konfiguration entsprechen:

- Bestätigen Sie mit `Y` oder `[Enter]`, um die Konfigurationsdateien mit den neuen Werten abzuspeichern.
  - ↳ Das Skript meldet die Speicherung der Konfigurationsdateien. Es gibt Informationen zum Umgang mit dem AntiVir Guard aus und fragt, ob der AntiVir Guard gestartet werden soll:

```
saving configuration to /etc/avguard.conf ... done
saving configuration to /etc/antivir.conf ... done

Running AvGuard
...
(Informationen zum AntiVir Guard)
...
Would you like to start AvGuard using the new config-
uration? [y]
```

- Geben Sie `Y` oder `[Enter]` ein, um den AntiVir Guard zu starten.

- ↳ Der AntiVir Guard wird gestartet. Wenn der AntiVir Guard bereits läuft, wird er automatisch neu gestartet, damit die neuen Einstellungen wirksam werden:

```
Starting AntiVir: avguard-server.
```

- ↳ Außerdem gibt das Skript Informationen zum Umgang mit dem Internet Updater aus und fragt, ob der Internet Updater gestartet werden soll:

```
Running Automatic Internet Updater
...
(Informationen zum Internet Updater)
...
Would you like to start the updater using the new con-
figuration? [y]
```

- ▶ Geben Sie `y` oder `[Enter]` ein, um den Internet Updater zu starten.
  - ↳ Der Internet Updater wird gestartet. Wenn der Internet Updater bereits läuft, wird er automatisch neu gestartet, damit die neuen Einstellungen wirksam werden. Damit ist die Konfiguration abgeschlossen.

```
Starting AntiVir: avupdater
Configuration Complete
```

- ↳ Abschließend wird die endgültige Zusammenfassung der Konfiguration angezeigt.

### 4.4 Konfigurieren der Nachrichten von AntiVir

#### Email-Versand bei Befall von Viren und unerwünschten Programmen anpassen

AntiVir kann eine Email verschicken, sobald ein Virus oder unerwünschtes Programm entdeckt wird.

- Rufen Sie configantivir auf:

```
/usr/lib/AntiVir/configantivir
```

- Bestätigen Sie die Einstellungen mit **[Enter]**, bis die Abfrage zur Email-Benachrichtigung kommt:

```
You may set AntiVir to send out an email message every  
time a concerning file is accessed. The message will  
also list the action that was taken to handle the  
file.
```

```
available options: y n
```

```
Would you like email notification of alerts? [n]
```

- Geben Sie hier **y** ein.

↳ Anschließend wird nach der Email-Adresse gefragt:

```
What email address will receive notifications?
```

- Geben Sie die Email-Adresse ein, z. B.

```
root@localhost
```

- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **[Enter]**.

Der Email-Versand ist konfiguriert.



Zusätzlich werden alle Meldungen über Updates von AntiVir an die angegebene Email-Adresse geschickt.

---

## Syslog-Meldungen spezifizieren

Für alle wichtigen Operationen gibt AntiVir Meldungen an den syslog-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird.



Wenn Sie keine Erfahrung mit dem syslog-Dämon haben, sollten Sie die voreingestellten Werte nicht ändern. Nähere Informationen zum syslog-Dämon entnehmen Sie bitte Ihrer UNIX-Dokumentation.

- Rufen Sie configantivir auf:

```
/usr/lib/AntiVir/configantivir
```

- Bestätigen Sie die Einstellungen mit `[Enter]`, bis die Abfrage zur Facility von syslog kommt:

```
Regardless of the other configuration options, Anti-
Vir will always log important information using sys-
log. Syslog uses two values to classify the
information to log: facility and priority. Facility
specifies the type of program making the log entry.
Priority specifies the importance of the log entry.
If you are unfamiliar with syslog then you may simply
accept the default values. However, it is encouraged
that you learn about syslog since it is used by many
services to log important events.
```

```
available FACILITIES: authpriv cron daemon kern lpr
mail news syslog user uucp
local0 local1 local2 local3 local4 local5 local6
local7
```

```
Which syslog FACILITY should AntiVir use? [user]
```

- Geben Sie die neue Facility ein.

↳ Anschließend wird nach der Priorität gefragt:

```
available PRIORITIES: emerg alert crit err warning
notice info debug
```

```
Which syslog PRIORITY should AntiVir use? [notice]
```

- Geben Sie die neue Priorität ein.
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.

Syslog ist konfiguriert.

### Logdatei von AntiVir anpassen

Zusätzlich zu syslog können alle Meldungen in eine separate Logdatei geschrieben werden.

- Rufen Sie configantivir auf:

```
/usr/lib/AntiVir/configantivir
```

- Bestätigen Sie die Einstellungen mit **[Enter]**, bis die Abfrage zur Logdatei kommt:

```
In addition to logging concerning activity through
syslog, you may also specify your own log file. This
can make it simpler to review past concerning activity
without having to sift through syslog files.
```

```
available options: y n
Would you like AntiVir to log to a custom file? [y]
```

- Geben Sie y ein.

↳ Anschließend wird nach dem Pfad der Logdatei gefragt:

```
What will be the log file name with absolute path (it
must begin with '/')
```

- Geben Sie den vollen Pfad der Logdatei ein, z. B.:

```
/var/log/antivir.log
```

- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **[Enter]**.

Die Logdatei ist konfiguriert.

## 4.5 Konfigurieren des residenten Wächters AntiVir Guard

### Überwachte Verzeichnisse definieren

Der AntiVir Guard kann beliebige, definierte Verzeichnisse ständig überwachen. Im Auslieferungszustand ist /home voreingestellt.



Auf das Verzeichnis /home mit seinen Unterverzeichnissen greifen die Nutzer üblicherweise zu, so dass hier die Gefahr eines Auftretens von Viren und unerwünschten Programmen am höchsten ist.

Auf die Systemverzeichnisse hat meist nur der Administrator Zugriff. Eine ständige Überwachung in diesen Verzeichnissen kostet unter Umständen unnötig Systemressourcen.

Der AntiVir Guard überwacht die eingestellten Verzeichnisse mit allen Unterverzeichnissen.

- Rufen Sie configavguard auf:

```
/usr/lib/AntiVir/configavguard
```

- Bestätigen Sie die Einstellungen mit , bis gefragt wird, ob die überwachten Verzeichnisse neu definiert werden sollen:

```
AvGuard gives you the option of specifying the paths
from which files will be scanned. All sub-directories
of specified paths will also be scanned as files are
accessed.
Current include paths = /home
```

```
available options: y n
Would you like to specify new include paths? [n]
```

- Geben Sie y ein.

↳ Anschließend wird nach den gewünschten Verzeichnispfaden gefragt:

```
Type in the paths one at time, pressing ENTER after
each path. All paths must be absolute (beginning with
'/'). When you are finished, simply enter a blank
line.
```

```
[IncludePath 1]
```

- Geben Sie die Verzeichnispfade einzeln ein. Bestätigen Sie jeden Verzeichnispfad mit . Nach dem letzten eingegebenen Pfad drücken Sie zweimal .



Die alte Liste von Verzeichnispfaden wird nicht ergänzt, sondern vollständig gelöscht. Sie müssen deshalb bei einer Neudefinition jedesmal die vollständige Liste aller neuen Pfade eingeben.

---

- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.

Die überwachten Verzeichnisse sind definiert.

### Ausgeschlossene Verzeichnisse definieren

Innerhalb der überwachten Verzeichnisse können beliebige Verzeichnisse von der Überwachung durch den AntiVir Guard ausgeschlossen werden. Dies ist z. B. für bestimmte temporäre Verzeichnisse sinnvoll, in denen AntiVir Dateien zum Scannen ablegt.



Wenn Sie AntiVir MailGate in Betrieb haben, darf der AntiVir Guard das Spool- und das temporäre Verzeichnis von MailGate nicht überwachen. Sonst blockiert der AntiVir Guard den Zugriff von MailGate auf Email-Attachments, die Viren oder unerwünschte Programme enthalten.

Falls die betroffenen Verzeichnisse in Ihren überwachten Verzeichnissen liegen (siehe [Überwachte Verzeichnisse definieren](#) – Seite 53), schließen Sie sie von der Überwachung aus.

---

Die Überwachung wird für die eingestellten Verzeichnisse mit allen Unterverzeichnissen ausgeschlossen.

- Rufen Sie `configavguard` auf:  
`/usr/lib/AntiVir/configavguard`
- Bestätigen Sie die Einstellungen mit `[Enter]`, bis gefragt wird, ob die ausgeschlossenen Verzeichnisse neu definiert werden sollen:

```
Unless under the specified included paths, files will
not be scanned. You may also want that particular sub-
directories within the included paths are also not
scanned.
For example, perhaps you want the entire /home direc-
tory scanned except for /home/bill. AvGuard allows you
to specify sub-directories of the included paths that
will not be scanned. These sub-directories are called
exclude paths. In this example /home/bill would be an
exclude path.
Current exclude paths = NONE

available options: y n
Would you like to specify new exclude paths? [n]
```

- Geben Sie `y` ein.



- ↳ Anschließend wird nach den gewünschten Verzeichnispfaden gefragt:

```
Type in the paths one at time, pressing ENTER after
each path. All paths must be absolute (beginning with
'/'). When you are finished, simply enter a blank
line.
```

```
[ExcludePath 1]
```

- Geben Sie die neuen Verzeichnispfade einzeln ein. Bestätigen Sie jeden Verzeichnispfad mit `[Enter]`. Nach dem letzten eingegebenen Pfad drücken Sie zweimal `[Enter]`.



Die alte Liste von Verzeichnispfaden wird nicht ergänzt, sondern vollständig gelöscht. Sie müssen deshalb bei einer Neudefinition jedesmal die vollständige Liste aller neuen Pfade eingeben.

- 
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.



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

---

Die ausgeschlossenen Verzeichnisse sind definiert.

### Kapazität des AntiVir Guard anpassen

Wenn mehrere Prozesse parallel auf Dateien zugreifen, können mehrere Dämonen des AntiVir Guard diese Zugriffe gleichzeitig überwachen. Das erhöht die Performance.

Die Anzahl der AntiVir Guard-Dämonen, die gleichzeitig laufen, kann zwischen 0 und 20 eingestellt werden.



Der voreingestellte Wert von 3 ist sinnvoll für kleinere Standardrechner. Für leistungsfähige Industrie-PC kann eine höhere Anzahl zweckmäßig sein, da hier häufiger auf Dateien gleichzeitig zugegriffen wird.

Andererseits sollten nicht mehr Dämonen laufen als unbedingt erforderlich, da ansonsten unnötig Arbeitsspeicher belegt wird.

- 
- Rufen Sie `configavguard` auf:  
`/usr/lib/AntiVir/configavguard`

↳ Die erste Abfrage betrifft bereits die Anzahl der Dämonen:

```
Files that are accessed by multiple processes at the
same time can be scanned by AvGuard in parallel. This
is accomplished by running multiple scanning daemons,
which allows your machine to run AvGuard with the
least amount of performance reduction.
```

```
A typical workstation only requires 3 daemons for
optimal performance. If you are running additional
servers (such as file, http, ftp, etc) then it is rec-
ommended that more daemons are used. You can disable
AvGuard by setting a value of 0 here.
```

```
available options: 0-20
```

```
How many daemons would you like to run? [3]
```

- ▶ Geben Sie die gewünschte Anzahl der Dämonen ein.
- ▶ Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `Enter`.

Die Kapazität des AntiVir Guard ist angepasst.

### Überwachungsmethode des AntiVir Guard anpassen

Der AntiVir Guard kann Dateien scannen, wenn sie geöffnet werden, wenn sie geschlossen werden und/oder wenn sie ausgeführt werden:

- Durch einen Scan beim Öffnen der Datei verhindert man, dass betroffene Dateien geöffnet, gelesen oder kopiert werden.
- Durch einen Scan beim Schließen der Datei verhindert man, dass betroffene Dateien geschrieben, gespeichert, kopiert oder aus dem Internet heruntergeladen werden. Sollte schädlicher Code enthalten sein, wird die konfigurierte Aktion (Reparatur, Umbenennen, Verschieben) ausgeführt.
- Durch einen Scan beim Ausführen der Datei verhindert man, dass sich Viren oder unerwünschte Programme durch die Ausführung eines Programms verbreiten.

Durch Scans beim Öffnen **und** beim Schließen erreicht man einen guten Schutz. Diese Konfiguration ist voreingestellt.



Werden Dateien nur beim Schließen gescannt, kann Folgendes passieren: In der kurzen Zeit zwischen dem Beschreiben und Schließen einer Datei ist ein Lesezugriff auf die Daten möglich, die konfigurierte Aktion wurde aber noch nicht ausgeführt. Deshalb empfehlen wir dringend, Dateien auch beim Öffnen zu scannen.

Beachten Sie auch, dass beim Einsatz des Linux-Kernels 2.6 mit seinem LSM Subsystem keine "close"-, sondern nur "open"-Events generiert werden. Dateien müssen deshalb unbedingt beim Öffnen gescannt werden.

---

- Rufen Sie configavguard auf:

```
/usr/lib/AntiVir/configavguard
```

- Bestätigen Sie die Einstellungen mit `[Enter]`, bis gefragt wird, ob Dateien beim Öffnen gescannt werden sollen:

```
Files may be scanned as they are opened. This is useful for preventing users from accessing concerning files. This includes opening, reading and copying concerning files.
```

```
available options: y n
```

```
Would you like to scan files as they are opened? [n]
```

- Geben Sie Y oder N ein, je nach der von Ihnen gewünschten Konfiguration.

- ↳ Anschließend wird gefragt, ob Dateien beim Schließen gescannt werden sollen:

```
Files may be scanned as they are closed. This is useful for preventing users from creating concerning files. This includes saving, downloading and copying concerning files.
```

```
available options: y n
```

```
Would you like to scan files as they are closed? [n]
```

- Geben Sie Y oder N ein, je nach der von Ihnen gewünschten Konfiguration.

- ↳ Anschließend wird gefragt, ob Dateien bei der Ausführung gescannt werden sollen:

```
Files may be scanned as they are executed. This is useful for preventing users from running concerning programs
```

```
available options: y n
```

```
Would you like to scan files as they are executed? [n]
```

- Geben Sie Y oder N ein, je nach der von Ihnen gewünschten Konfiguration.



Wenn Sie alle Abfragen mit N beantworten, wird der AntiVir Guard deaktiviert.

---

- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.

Die Überwachungsmethode des AntiVir Guard ist angepasst.

### Dateien während des Zugriffs reparieren

Normalerweise blockiert der AntiVir Guard den Zugriff auf eine Datei, die einen Virus oder ein unerwünschtes Programm enthält.

Der AntiVir Guard ist in der Lage, Dateien während des Zugriffs zu reparieren. Wenn die Reparatur möglich ist, kann der Benutzer gefahrlos auf die reparierte Datei zugreifen. Wenn die Reparatur nicht möglich ist, bleibt der Zugriff blockiert.

Der Vorgang wird in jedem Fall in der Logdatei protokolliert.

- Rufen Sie configavguard auf:

```
/usr/lib/AntiVir/configavguard
```

- Bestätigen Sie die Einstellungen mit , bis gefragt wird, ob betroffene Dateien repariert werden sollen:

```
If an concerning file is found, AvGuard can try to
remove the problem. If the problem cannot be removed,
access to the file will still be blocked. However, if
the problem can be removed, the user will be allowed
normal access.
```

```
available options: y n
```

```
Would you like to try to repair concerning files? [y]
```

- Geben Sie `y` ein, um die Reparatur betroffener Dateien zu ermöglichen.
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit .

Der AntiVir Guard repariert ab jetzt betroffene Dateien beim Zugriff.

## Betroffene Dateien automatisch umbenennen oder verschieben

Wenn eine Datei nicht während des Zugriffs repariert werden kann, oder wenn diese Option nicht eingestellt ist, kann der AntiVir Guard die betroffene Datei automatisch umbenennen oder verschieben.

Der Zugriff des Benutzers auf diese Datei bleibt dabei natürlich blockiert. Der Vorgang wird in jedem Fall in der Logdatei protokolliert.

- Rufen Sie configavguard auf:

```
/usr/lib/AntiVir/configavguard
```

- Bestätigen Sie die Einstellungen mit **[Enter]**, bis gefragt wird, wie der AntiVir Guard auf betroffene Dateien reagieren soll:

```
When an alert is found and cannot be removed, there
are several ways in which AvGuard can respond.
log only - the name of the concerning file will only
           be logged using syslog
rename   - the concerning file will be renamed to
           have a .XXX extension
move     - the concerning file will be moved to a
           directory of your choice
Regardless of which option you choose, the event
involving the concerning file will be logged using
syslog and access to the file will be blocked.

available options: l r m
How should concerning files be handled? [l]
```

Betroffene  
Dateien  
umbenennen

Wenn betroffene Dateien umbenannt werden sollen:

- Geben Sie **R** ein.
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **[Enter]**.

Ab jetzt wird an betroffene Dateien die Endung **.XXX** angehängt.

Betroffene  
Dateien  
verschieben

Wenn betroffene Dateien verschoben werden sollen:

- Geben Sie **M** ein.
- ↳ Anschließend wird gefragt, in welches Verzeichnis betroffene Dateien verschoben werden sollen:

```
Which directory should they be moved to? []
```

- Geben Sie den vollständigen Pfad des Verzeichnisses ein, z. B.:  
`/home/quarantine`
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **[Enter]**.

Ab jetzt werden betroffene Dateien in das angegebene Verzeichnis verschoben.



Das Verzeichnis sollte ausschließlich zum Ablegen betroffener Dateien verwendet werden ("Quarantäneverzeichnis").

---



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

---

Keine  
Aktionen

Wenn betroffene Dateien weder umbenannt noch verschoben werden sollen:

- ▶ Geben Sie `L` ein.
- ▶ Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.

Ab jetzt bleiben die Dateien unter gleichem Namen im gleichen Verzeichnis. Der Zugriff bleibt aber blockiert und der Vorgang wird protokolliert.

## Scannen gepackter Archive konfigurieren

Der AntiVir Guard kann in komprimierten Dateien (z. B. `.zip`, `.gz`, `.tar`) nach Viren und unerwünschten Programmen suchen. Hierfür werden die Dateien dekomprimiert und gescannt.

Zusätzlich können folgende Optionen eingestellt werden:

- Maximale entpackte Größe der komprimierten Dateien. Der AntiVir Guard scannt dann nur Dateien, die im entpackten Zustand nicht größer als dieser Wert sind. Es gibt komprimierte Dateien, die keinen sinnvollen Inhalt haben, aber bewusst so angelegt sind, dass sie sich auf eine "unsinnige Größe" aufblähen, um den Rechner lahm zu legen. Diese Option schützt vor dem Entpacken solcher Archivdateien.
  - Vorgegebener Wert: 1 Gigabyte (1073721824 Byte)
- Maximale Rekursionstiefe der komprimierten Dateien. Gepackte Dateien können ihrerseits wieder gepackt sein usw. Der AntiVir Guard scannt dann nur Dateien, bei denen die Rekursionstiefe nicht größer als der eingestellte Wert sind. Hierdurch lässt sich Zeit sparen.
  - Vorgegebener Wert: 5
- ▶ Rufen Sie `configavguard` auf:  
`/usr/lib/AntiVir/configavguard`

- Bestätigen Sie die Einstellungen mit `[Enter]`, bis gefragt wird, ob komprimierte Dateien gescannt werden sollen:

```
There may be alerts hiding within compressed files
(.zip, .gz, .tar, etc). You may configure AvGuard so
that these compressed files are decompressed and
searched for concerning files. This will help to
ensure that your server is free from unwanted files.
```

```
available options: y n
Would you like to scan compressed files? [n]
```

- Geben Sie `y` ein, um komprimierte Dateien zu scannen.
  - ↳ Anschließend wird nach der maximalen entpackten Größe der komprimierten Dateien gefragt:

```
In order to scan the contents of compressed files, the
files must be decompressed. For very large compressed
files it could take a long time to decompress every-
thing. For this reason, you may wish you put a size
limit for compressed files that will be scanned. The
size limit is given in bytes. For example, 1 gigabyte
= 1073741824 bytes. You may set this value to 0 to
have no limit on the size of scanned compressed files.
```

```
available options: 0-??
What is the maximum size compressed file (in bytes)
to be scanned? [1073741824]
```

- Geben Sie die maximale entpackte Größe in Bytes ein. Wenn alle gepackten Dateien unabhängig von der Größe gescannt werden sollen, geben Sie `0` ein.

- ↳ Anschließend wird nach der maximalen Rekursionstiefe der komprimierten Dateien gefragt:

It is possible that a compressed file has many compressed files as contents. For example, inside of filename.zip there may be a file1.zip file. Each compressed file within a compressed file is referred to as a recursion level. If AvGuard should decompress apple.zip it must scan recursion level 1. If it is supposed to also decompress seed.zip, it must scan recursion level 2.

Since decompressing takes extra time, you may wish to set a limit on the recursion level that will be scanned. A value of 0 means that there will be no limit.

available options: 0-??

What is the maximum recursion level in compressed files to be scanned? [5]

- ▶ Geben Sie die maximale Rekursionstiefe ein. Wenn alle gepackten Dateien unabhängig von der Rekursionstiefe gescannt werden sollen, geben Sie 0 ein.
- ▶ Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **[Enter]**.

Das Scannen gepackter Dateien ist konfiguriert.



## 4.6 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 17 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.

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	<p><b>Einträge über Dateizugriffe im Log:</b></p> <p>samba-vscan kann jeden Dateizugriff im Log vermerken (wenn dieser Wert auf <code>yes</code> gestellt wird) oder nur die Zugriffe auf Dateien, in denen ein Virus bzw. unerwünschtes Programm entdeckt wurde (<code>no</code>). Die Voreinstellung ist <code>no</code>.</p> <pre>verbose file logging = no</pre>
scan on open/ scan on close	<p><b>Dateien beim Öffnen und/oder Schließen untersuchen:</b></p> <p>samba-vscan kann Dateien beim Öffnen und/oder Schließen auf verschiedene Ereignisse hin untersuchen (Voreinstellung: in beiden Fällen).</p> <pre>scan on open = yes scan on close = yes</pre>
deny access on error/ deny access on minor error	<p><b>Zugriff auf Dateien verweigern:</b></p> <p>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:</p> <p>Ist der Scanner selbst nicht verfügbar, gilt das als Fehler.</p> <p>Ist der Scanner zwar erreichbar, konnte aber die Datei nicht scannen, gilt das als ein minderer Fehler.</p> <p>Weil in diesen Situationen Schadsoftware unerkannt ins System gelangen kann, wird standardmäßig auch in diesen Fällen der Zugriff verweigert.</p> <pre>deny access on error = yes deny access on minor error = yes</pre>
send warning message	<p><b>Nachricht bei verweigertem Zugriff auf Datei:</b></p> <p>samba-vscan kann bei verweigertem Zugriff auf eine Datei den entfernten Nutzer des Dateiservers per Popup benachrichtigen (Voreinstellung: <code>yes</code>).</p> <pre>send warning message = yes</pre>
concerning file action (infected file action)	<p><b>Datei-Aktionen:</b></p> <p>samba-vscan kann nicht nur den Zugriff auf betroffene Dateien verweigern, sondern auch zusätzliche Aktionen auslösen:</p> <ul style="list-style-type: none"><li>• Löschen der Datei</li><li>• Verschieben der Datei in einen Quarantäne-Bereich</li></ul> <p>Die entsprechenden Werte für diese Option sind <code>nothing</code> (Voreinstellung), <code>delete</code> und <code>quarantine</code>.</p>



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 life-  
time

### **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  
name

### **Pfad für antivir-Programm:**

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

### **Archive prüfen:**

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.

## 4.7 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 83.

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

1. Sie verwenden den mitgelieferten Internet Updater, den Sie einfach konfigurieren können. Dies ist empfohlen, wenn Sie geringe UNIX-Kenntnisse haben und wenig eigene Anpassungen vornehmen möchten.
2. 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:

```
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 des Proxyservers gefragt:

```
What is the HTTP proxy server name? []
```

- Geben Sie den Namen ein, z. B.:  
`proxy.domain.com`
  - ↳ Anschließend wird nach dem Port des Proxyservers gefragt:

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

- Geben Sie den Port ein, z. B.:  
`8080`
  - ↳ Anschließend wird gefragt, ob für den Proxyserver ein Username und ein Passwort notwendig sind:

```
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/pass-
word? [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.
- Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit `[Enter]`.

Der Internet-Zugang für Updates ist konfiguriert.

## Automatische Updates über den Internet Updater konfigurieren

Der Internet Updater ist ein sehr einfacher Dämon, der in festgesetzten Abständen folgenden Befehl aufruft:

```
antivir --update
```



Damit die nachfolgenden Einstellungen wirksam werden können, muss der Internet Updater installiert sein. Wenn Sie die Installation wie unter [AntiVir installieren](#) – Seite 20 beschrieben vorgenommen haben, ist dies auch der Fall. Ansonsten müssen Sie nochmals das Installationsskript laufen lassen, siehe [AntiVir erneut installieren](#) – Seite 28.

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
```

↳ Die erste Abfrage betrifft bereits die Häufigkeit der Updates:

```
AntiVir is equipped with an Automatic Internet
Updater. At specified intervals, AntiVir will connect
to an updater server to check for newer versions of
the AntiVir engine or the virus data file. 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 cur-
rent against virus attacks.
```

```
AntiVir can be configured to check for updates every 2
hours (2) or once a day (d). You can also choose to
have the Automatic Internet Updater never check (n).
```

```
available options: 2 d n
```

```
How often should AntiVir check for updates? [n]
```

► 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:

The Automatic Internet 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? [16:00]

- ▶ 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 .

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

### Internet Updater manuell starten und anhalten

Wenn Sie den Internet Updater starten wollen:

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

Wenn Sie den Internet Updater anhalten wollen:

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

Wenn Sie den aktuellen Status des Internet Updater 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 regelmäßige 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 Updater.

- 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 76

## Internet Updater automatisch starten

Wenn Sie nicht mit dem Cron-Dämon arbeiten wollen, benutzen Sie den Internet Updater. Wenn Sie die Installation so vorgenommen haben, wie in [AntiVir installieren](#) – Seite 20 beschrieben, ist Ihr System schon entsprechend eingestellt.

Wenn der Internet Updater noch nicht automatisch beim Systemstart gestartet wurde:

- ▶ Führen Sie eine [AntiVir erneut installieren](#) – Seite 28 mit den entsprechenden Einstellungen durch.

### Authentizität der Updates durch GnuPG sicherstellen

GnuPG ist eine kostenlose Alternative zum Verschlüsselungsprogramm PGP (Pretty Good Privacy). Mit GnuPG kann die Authentizität der Updates von AntiVir sichergestellt 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 support@antivir.de
```

↳ 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 AntiVir-Webseite (<http://www.antivir.de>) angezeigt.
- ▶ Unterschreiben Sie den öffentlichen AntiVir-PGP-Schlüssel, um seine Gültigkeit zu beglaubigen:  

```
gpg --sign-key support@antivir.de
```

- Wechseln Sie in das Unterverzeichnis `/bin` Ihres AntiVir-Installationsverzeichnisses, 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/antivir.conf` im Eintrag `GnuPGBinary` den vollen Pfad zur GnuPG-Binärdatei ein, z. B.:

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



Diese Option kann nur manuell in `antivir.conf` editiert werden. Eine Einstellung über die Konfigurationsskripte ist nicht möglich, um die Gefahr einer fehlerhaften Konfiguration zu mindern.

---

- Starten Sie den Internet Updater neu, um die geänderten Einstellungen in `antivir.conf` wirksam werden zu lassen:

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

Die Authentizität der Updates wird ab jetzt durch GnuPG sichergestellt.

### 4.8 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 39)
- ▶ 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 37 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 75 erhalten Sie einen Überblick über sämtliche Optionen des Kommandozeilenscanners.
- In [AntiVir Kommandozeilenscanner in der Anwendung](#) – Seite 81 werden exemplarische Anwendungen des Kommandozeilenscanners aufgeführt.
- In [Vorgehen bei Fund eines Virus/unerwünschten Programms](#) – Seite 86 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                | Alle Dateien werden gescannt, nicht nur Programmdateien                                                                                                                |
| --alltypes                | Sucht neben Viren auch nach unerwünschten Programmen. Diese Option ist eine Abkürzung, die für alle möglichen --with-<type> Optionen steht                             |
| --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: /etc/antivir.conf                                                                                                               |
| --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 |
| -cf<dateiname>            | Gescannte Dateien der CRC-Datenbank <dateiname> hinzufügen.<br>Siehe <a href="#">CRC-Datenbank verwenden</a> – Seite 85                                                |
| -cn                       | Nur in Verbindung mit -cf verwendbar.<br>Siehe <a href="#">CRC-Datenbank verwenden</a> – Seite 85                                                                      |
| -cu                       | Nur in Verbindung mit -cf verwendbar.<br>Siehe <a href="#">CRC-Datenbank verwenden</a> – Seite 85                                                                      |
| -cv                       | Nur in Verbindung mit -cf verwendbar.<br>Siehe <a href="#">CRC-Datenbank verwenden</a> – Seite 85                                                                      |
| -del                      | Bei einem Fund werden betroffene Dateien gelöscht                                                                                                                      |
| -dmdas                    | Alle Makros eines Dokuments werden gelöscht, wenn eins verdächtig erscheint                                                                                            |
| -dmddel                   | OLE-Dokumente mit verdächtigen Makros werden gelöscht                                                                                                                  |

| Option             | Funktion                                                                                                                                       |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| -dmse              | Der Exit-Code von antivir wird auf 101 gesetzt, wenn ein Makro gefunden wird                                                                   |
| -e -del            | Bei einem Fund werden betroffene Dateien repariert, wenn möglich. Wenn keine Reparatur möglich ist, werden betroffene Dateien gelöscht.        |
| -e -ren            | Bei einem Fund werden betroffene Dateien repariert, wenn möglich. Wenn keine Reparatur möglich ist, werden betroffene Dateien umbenannt.       |
| --exclude=<dir>    | Ignoriert das angegebene Verzeichnis beim Scannen und durchsucht Dateien unterhalb dieses Verzeichnisses nicht                                 |
| --help             | Alle möglichen Optionen werden ausgegeben                                                                                                      |
| --heur-macro       | Aktiviert die Heuristik für Makroviren in Dokumenten                                                                                           |
| --heur-nomacro     | Deaktiviert die Heuristik für Makroviren in Dokumenten                                                                                         |
| --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 aufgenommener unerwünschter Programme aus             |
| -kf<dateiname>     | AntiVir verwendet die unter <dateiname> angegebene Lizenzdatei                                                                                 |
| -lang:DE           | AntiVir gibt deutsche Texte aus                                                                                                                |
| -lang:EN           | AntiVir gibt englische Texte aus                                                                                                               |
| --log-email=<addr> | Sendet einen Report über diesen Scan-Durchlauf per Email an die angegebene Adresse (zusätzlich zur Ausgabe am Bildschirm)                      |
| -noboot            | Die Bootsektorprüfung wird abgeschaltet. Hiermit kann bei gezielten Suchläufen Zeit gespart werden, ansonsten wird die Option nicht empfohlen. |

| Option         | Funktion                                                                                                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -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 Suchläufen 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                                                                                                                                                  |
| -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: <ul style="list-style-type: none"><li>– %d: Tag</li><li>– %m: Monat</li><li>– %y: Jahr</li></ul> |
| -ro            | Die Logdatei überschreibt die bestehende Logdatei                                                                                                                                                                        |
| -rs            | Meldungen über Viren und unerwünschte Programme werden einzellig ausgegeben                                                                                                                                              |
| -s             | Alle Unterverzeichnisse werden durchsucht                                                                                                                                                                                |



| Option                            | Funktion                                                                                                                                                                                                                     |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--scan-in-archive</code>    | Auch Inhalte von gepackten Archiven werden gescannt                                                                                                                                                                          |
| <code>--scan-in-mbox</code>       | Auch Inhalte von scannten werden gescannt                                                                                                                                                                                    |
| <code>--temp=&lt;dir&gt;</code>   | AntiVir legt seine temporären Dateien in <dir> ab                                                                                                                                                                            |
| <code>--update</code>             | AntiVir führt ein Update seiner eigenen Dateien durch, um den Schutz vor Viren und unerwünschten Programmen wieder auf den neuesten Stand zu bringen                                                                         |
| <code>-v</code>                   | Ein Intensiv-Scan wird durchgeführt. AntiVir prüft komplette Dateien. Möglicherweise werden hierbei auch Fehlermeldungen ausgegeben. Diese Option sollte nur im Ausnahmefall gewählt werden, z. B. nach einem Fund.          |
| <code>--version</code>            | Die Version von AntiVir wird angezeigt                                                                                                                                                                                       |
| <code>--warnings-as-alerts</code> | 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                             |
| <code>--with-&lt;type&gt;</code>  | Aktiviert die Erkennung von unerwünschten Programmen, die keine Viren sind. <type> kann eine der Varianten dialer, game, joke oder pms sein. Die Option kann mehrfach angegeben werden (siehe auch <code>--alltypes</code> ) |
| <code>-z</code>                   | Entspricht der Option <code>--scan-in-archive</code>                                                                                                                                                                         |
| <code>@&lt;rspdatei&gt;</code>    | AntiVir liest Parameter aus der Datei <rspdatei>. In <rspdatei> 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 <code>antivir.vdf</code> konnte nicht gelesen werden                                                    |
| 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 |
| $\geq 2$  | 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:

1. Durch den AntiVir Guard, wenn die Datei durch den AntiVir Kommandozeilenscanner geöffnet wird
2. 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:

- |            |                                                               |
|------------|---------------------------------------------------------------|
| --allfiles | Scannt alle Dateien                                           |
| --alltypes | Erkennt alle Arten von verdächtigen und unerwünschten Dateien |
| -s         | Scannt alle Unterverzeichnisse                                |
| -z         | Scannt auch gepackte Dateien                                  |

► Geben Sie ein:

```
antivir --allfiles -s -z --alltypes /
```

### 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:

|            |                                |
|------------|--------------------------------|
| --allfiles | Scannt alle Dateien            |
| -s         | Scannt alle Unterverzeichnisse |
| -z         | 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 --allfiles -s -z /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:

|            |                                                                           |
|------------|---------------------------------------------------------------------------|
| --allfiles | Prüft alle Dateien                                                        |
| -del       | Löscht betroffene Dateien                                                 |
| -e -del    | 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 --allfiles -del /home/myhome
```

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

► Geben Sie ein:

```
antivir --allfiles -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-Dämonen (z. B. den AntiVir Guard, SAVAPI, 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 nicht die notwendigen Rechte, um die AntiVir-Dämonen neu zu starten. Der Neustart muss dann von **root** 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 Kommandozeilen-scanner in ein Skript integrieren und die [Exit-Codes](#) – Seite 79 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 -----
```

## CRC-Datenbank verwenden

AntiVir bietet die Möglichkeit, eine Datenbank mit den CRC-Werten der gescannten Dateien zu erstellen und zukünftige Scans mit dieser Datenbank abzugleichen. Standardmäßig werden hierfür die ersten 16 Bytes einer Datei verwendet.

AntiVir vergleicht also für Dateien, deren CRC-Wert in der Datenbank abgelegt ist, lediglich den aktuellen CRC-Wert der Datei mit dem Wert in der Datenbank. Nur bei einer Abweichung wird die Datei gescannt. Auf diese Weise wird erreicht, dass AntiVir nur veränderte oder neue Dateien scannt.

Hierfür bietet AntiVir folgende Optionen

- cf<dateiname> -cn CRC-Werte gescannter Dateien der CRC-Datenbank <dateiname> hinzufügen. Über diese Option wird die Datenbank auch beim ersten Mal aufgebaut
- cf<dateiname> Beim Scannen zunächst CRC-Wert der Datei mit dem gespeicherten Wert in der CRC-Datenbank <dateiname> vergleichen und nur bei einer Abweichung den Scan durchführen
- cf<dateiname> -cu CRC-Werte der gescannten Dateien in der CRC-Datenbank aktualisieren
- cv Nur in Verbindung mit -cf verwendbar. Zum Erzeugen des CRC-Wertes die gesamte Datei und nicht nur die ersten 16 Bytes verwendet. Sicherer, aber langsamer

**Beispiel** Wenn Sie eine CRC-Datenbank antivir.db von allen Dateien neu anlegen wollen:

► Geben Sie ein:

```
antivir -cf/var/tmp/antivir.db -cn --allfiles -s /
```

Wenn Sie einen Suchlauf über alle Dateien unter Verwendung der CRC-Datenbank durchführen wollen:

► Geben Sie ein:

```
antivir -cf/var/tmp/antivir.db --allfiles -s /
```

### 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 H+BEDV Datentechnik 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@antivir.de](mailto:virus@antivir.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 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 COMMERCIAL-Lizenz für AntiVir UNIX Server vorhanden sein (`antivir --version`).
- In der Datei `antivir.conf` muss der Parameter für `GuiSupport` gesetzt sein.
- Der Benutzer muss in der "antivir"-Gruppe sein.

Sind diese Bedingungen nicht erfüllt, erscheint die Meldung, dass AntiVir UNIX Server steht oder dass AntiVir UNIX Server nicht auf dem Rechner vorhanden ist.

## 6.2 AntiVir Scanner

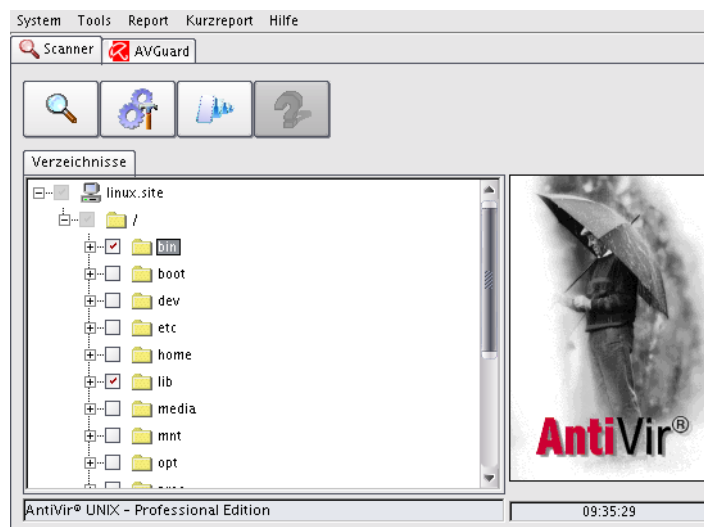
### 6.2.1 AntiVir Scanner über GUI bedienen

#### GUI starten

- Starten Sie die GUI:

```
/usr/lib/AntiVir/antivir-gui
```

↳ Die GUI erscheint mit dem Dialogfenster **Verzeichnisse**.



#### Symbolleiste



Anklicken schaltet in das Dialogfenster des Scanvorgangs und startet diesen.



Anklicken schaltet in das Dialogfenster **Konfiguration** um.



Anklicken öffnet das Dialogfenster **Report** um.

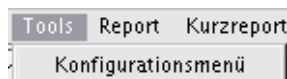
## Menüleiste

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



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

Report



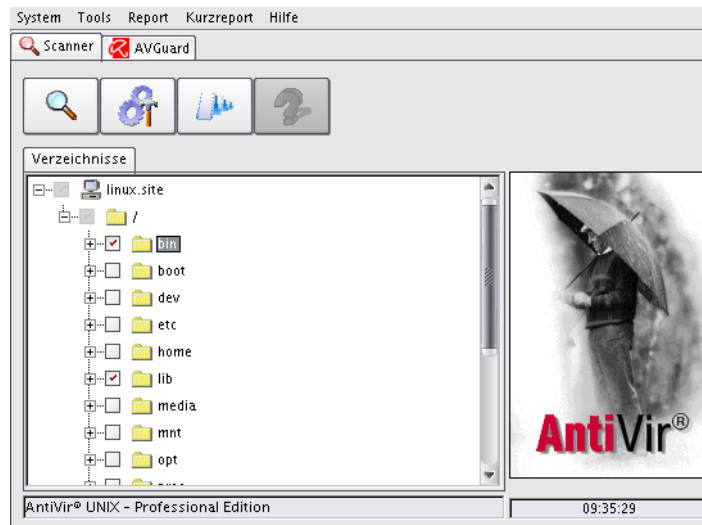
- **Report anzeigen:** Öffnet ein Dialogfenster, in dem der Inhalt der Reportdatei angezeigt wird (avscanner.log)
- **Report Einstellungen:** Öffnet das Dialogfenster **Konfiguration**, Bereich **Report**
- **Report löschen:** Löscht die im Bereich **Report** des Konfigurationsdialogs angegebene Reportdatei

Kurzreport



- **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.



Letzte  
Meldung

Anzeige des zuletzt gefundenen Virus bzw. unerwünschten Programms

Anzahl  
Dateien

Anzahl der aktuell gescannten Dateien

|           |                                |
|-----------|--------------------------------|
| Zeit      | Dauer des Suchvorgangs         |
| Warnungen | Anzahl der aktuellen Warnungen |
| Funde     | Anzeige der aktuellen Alarme   |
| Ordner    | Aktuell gescanntes Verzeichnis |
| Datei     | Aktuell gescannte Datei        |
| Status    | Anzeige des Status             |

### 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.

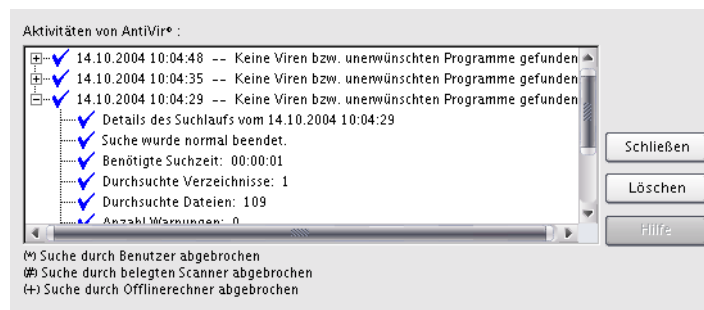
- Klicken Sie auf die Schaltfläche **Stop**.
  - ↳ Der Scanvorgang wird beendet.
  - ↳ Das Dialogfenster **Status** mit einer Zusammenfassung des Scanvorgangs erscheint.

### Kurzreport anzeigen

- Klicken Sie in der Menüleiste **Kurzreport/Kurzreport anzeigen....**
  - ODER –

Wenn das Dialogfenster **Status** am Ende eines Scanvorgangs erscheint:

- Klicken Sie auf die Schaltfläche **Kurzreport**.
  - ↳ 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.

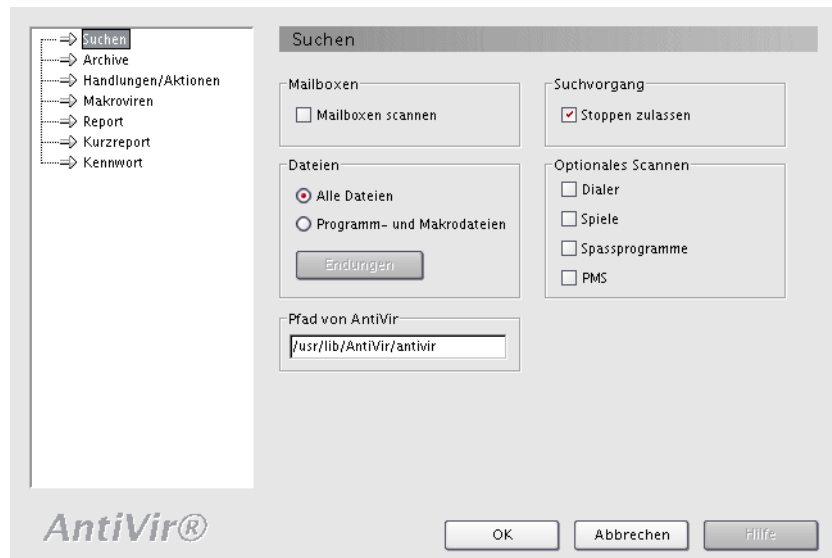
Wenn Sie die Kurzreports löschen wollen:

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

### 6.2.2 AntiVir Scanner über GUI konfigurieren



- Klicken Sie auf die Schaltfläche **Einstellungen**.
  - ODER –
  - Klicken Sie in der Menüleiste auf **Tools/Konfigurationsmenü**.
  - ↳ Das Dialogfenster **Konfiguration** erscheint:



- Klicken Sie auf den gewünschten Eintrag der Liste.
  - ↳ Das jeweilige Dialogfenster erscheint.

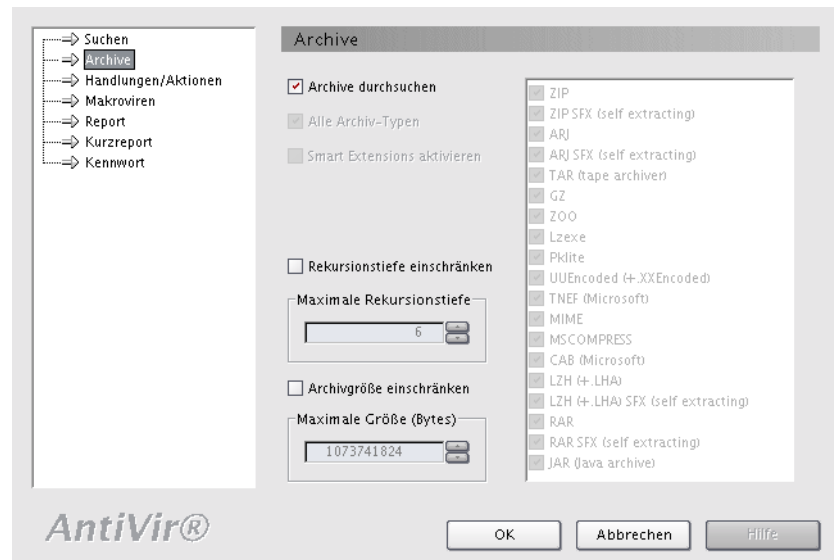
#### Bereich Suchen

Hier legen Sie das grundlegende Verhalten der Suchroutine fest.

- |                    |                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mailboxen          | Wenn die Inhalte Ihrer Mailboxen gescannt werden sollen: <ul style="list-style-type: none"><li>► Aktivieren Sie das Kontrollkästchen <b>Mailboxen scannen</b>.</li></ul>                                 |
| Dateien            | Je nachdem, ob alle Dateien oder nur Programm- und Makrodateien gescannt werden sollen: <ul style="list-style-type: none"><li>► Aktivieren Sie das entsprechende Optionsfeld.</li></ul>                  |
| Pfad von AntiVir   | Im Eingabefeld <b>Pfad von AntiVir</b> befindet sich der Pfad, in dem AntiVir installiert wurde. In der Regel liegt die Programmdatei in:<br><code>/usr/lib/AntiVir/antivir</code>                       |
| Suchvorgang        | Wenn Sie einen manuellen Abbruch des Suchvorgangs zulassen wollen: <ul style="list-style-type: none"><li>► Aktivieren Sie das Kontrollkästchen <b>Stoppen zulassen</b>.</li></ul>                        |
| Optionales Scannen | Wenn auch nach Dialern, Spielen, Spaßprogrammen oder PMS gesucht werden soll (siehe Anhang): <ul style="list-style-type: none"><li>► Aktivieren Sie das/die entsprechende(n) Kontrollkästchen.</li></ul> |



## Bereich Archive



Archive  
durchsuchen

Wenn Archive durchsucht werden sollen:

- Aktivieren Sie das Kontrollkästchen **Archive durchsuchen**.

Wenn Sie dieses Kontrollkästchen nicht aktiviert haben, sind die folgenden Optionen nicht verfügbar.

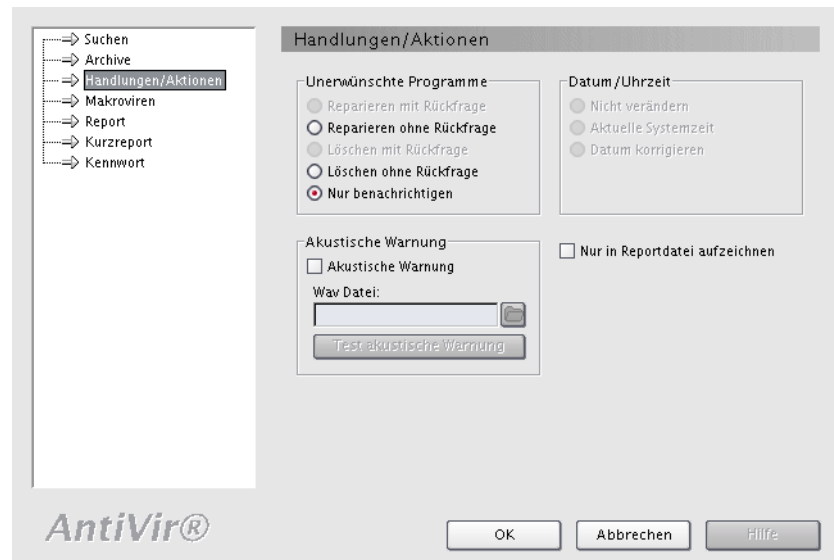
Rekursions-  
tiefe

- Aktivieren Sie ggf. das Kontrollkästchen **Rekursionstiefe einschränken** und geben Sie einen Wert an.

Archivgröße

- Aktivieren Sie ggf. das Kontrollkästchen **Archivgröße einschränken** und geben Sie einen Wert an.

### Bereich Handlungen/Aktionen



Uner-  
wünschte  
Programme

Folgende Optionen stehen Ihnen zur Verfügung:

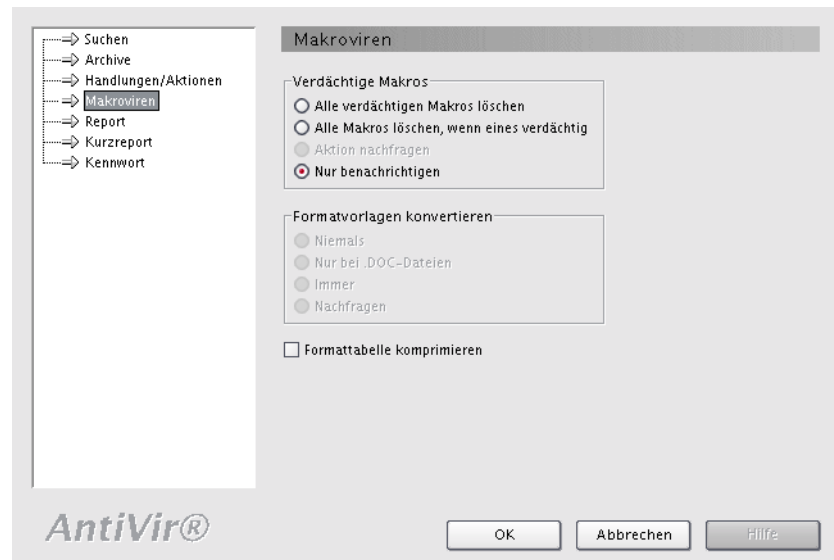
- Reparieren ohne Rückfrage
- Löschen ohne Rückfrage
- Nur benachrichtigen

► Aktivieren Sie das entsprechende Optionsfeld.

Akustische  
Warnung

► Aktivieren Sie ggf. das Kontrollkästchen **Akustische Warnung** und geben Sie eine Wave-Datei zum Abspielen an.

### Bereich Makroviren

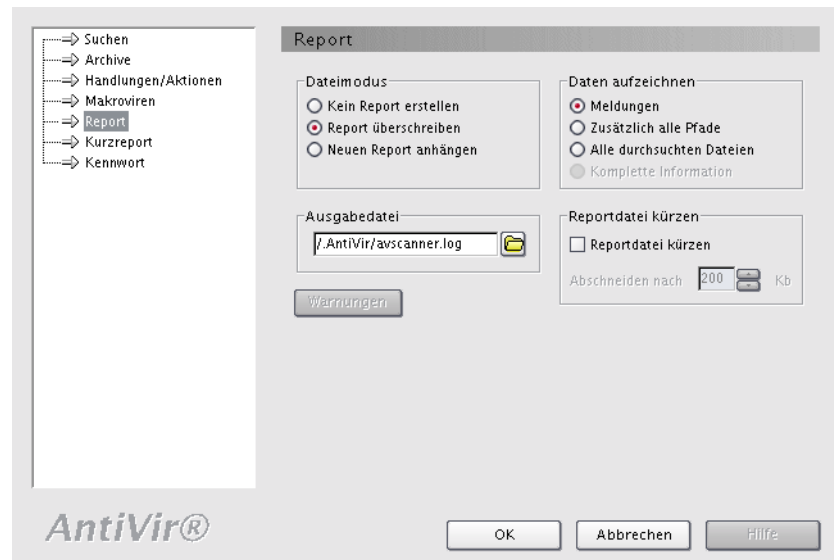


Verdächtige  
Makros

Folgende Optionen stehen Ihnen zur Verfügung:

- Alle verdächtigen Makros löschen
  - Alle Makros löschen, wenn eines verdächtig
  - Nur benachrichtigen
- Aktivieren Sie das entsprechende Optionsfeld.

### Bereich Report

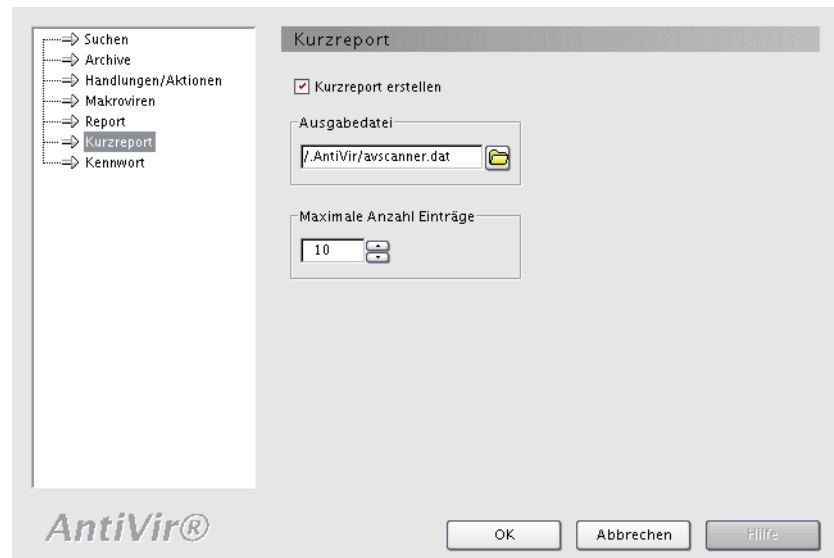


**Dateimodus** Die Meldungen des Kommandozeilenscanners werden in einer Reportdatei gesammelt. Folgende Optionen stehen Ihnen zur Verfügung:

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

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

## Bereich Kurzreport



Kurzreport  
erstellen

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.

## Bereich Kennwort

Sie können ein Kennwort festlegen, um die Optionen der GUI zu sichern. Das Kennwort wird dann bei jedem Öffnen des Dialogfensters Konfiguration verlangt.



- ▶ Geben Sie ggf. ein Kennwort ein und bestätigen Sie es.

### 6.3 AntiVir Guard

#### 6.3.1 AntiVir Guard über GUI bedienen

##### GUI starten

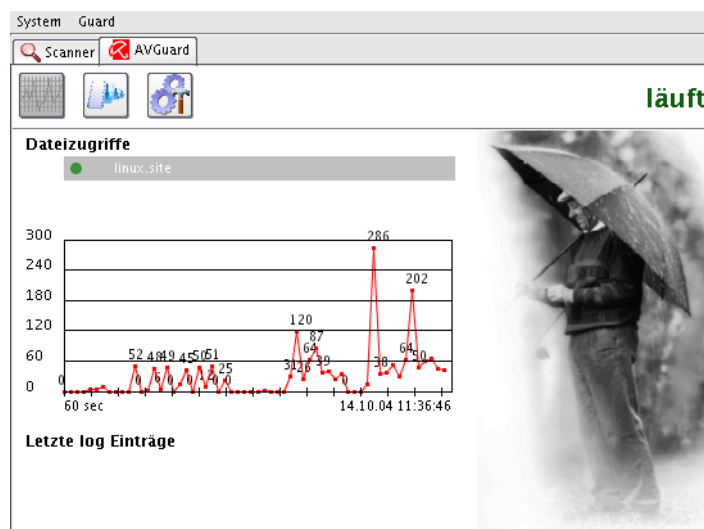
- ✓ Damit AntiVir Guard mit der GUI kommuniziert, muss der Eintrag **GuiSupport** in **avguard.conf** aktiviert sein.

- Starten Sie die GUI:

`/usr/lib/AntiVir/antivir-gui`

↳ Die GUI erscheint mit dem Dialogfenster **Verzeichnisse**.

- Klicken Sie auf den Reiter **AVGuard**.



##### 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



- **Log Datei:** 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 100

Im Dialogfenster **Echtzeit Status** werden die aktuellen Dateizugriffe angezeigt, z. B. 286 Dateien/Sekunde. Die y-Achse ändert sich automatisch in Abhängigkeit des jeweiligen Höchstwertes.

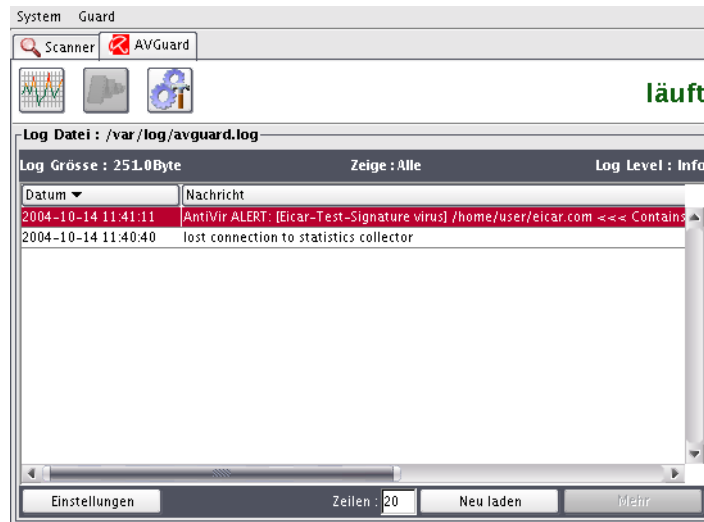
Status anzeigen

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:

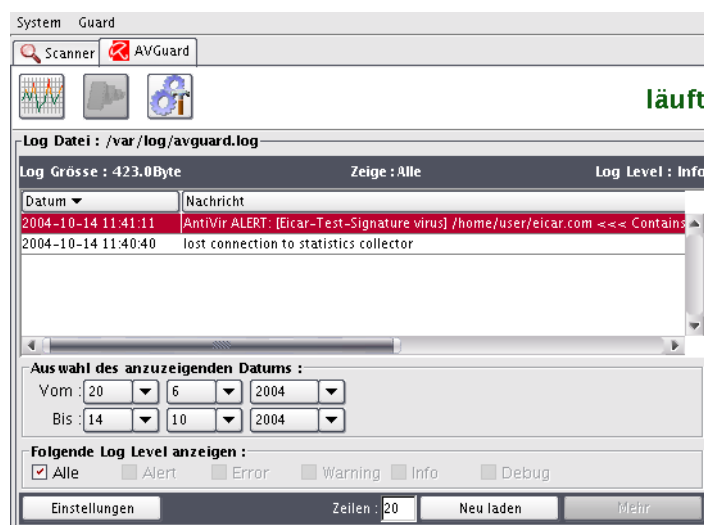


Logdatei Zeigt die komplette Logdatei mit Angabe des Pfads an, darunter die aktuelle Größe der Logdatei in KB, welche Log Level angezeigt werden und welchen Log Level der AntiVir Guard verwendet.

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 104

### 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 38 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:

#### Bereich Basis

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 (siehe [Ausgeschlossene Verzeichnisse definieren](#) – Seite 54). 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**.

Scannen ...

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.

**Archive scannen** Der AntiVir Guard scannt zusätzlich komprimierte Archive beim Zugriff, abhängig von den Einstellungen im Bereich **Erweitert**.

In der Voreinstellung ist diese Option deaktiviert, um die Performance von AntiVir möglichst hoch zu halten.

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

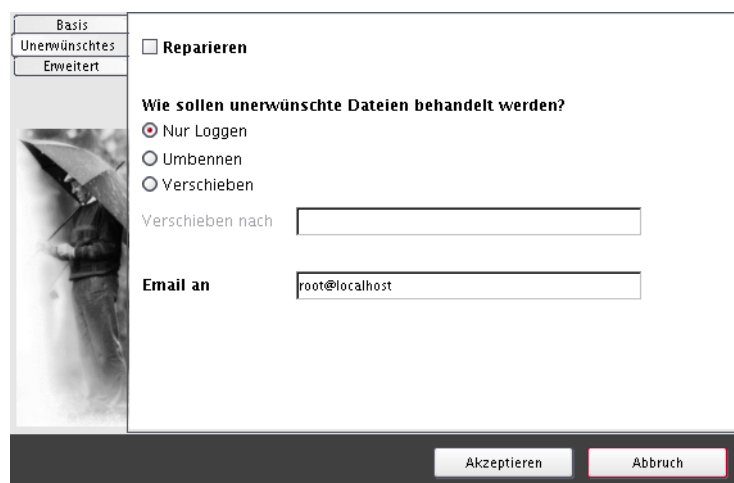
Wenn Archive bei der Suche berücksichtigt werden sollen:

- Aktivieren Sie das Optionsfeld **Ja**.

**Optionales Scannen** Wenn der AntiVir Guard nicht nur nach Viren, sondern auch nach unerwünschten Programmen (Dialer, Games, Jokes, PMS) suchen soll:

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

### Bereich Unerwünschtes



**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 unerwünschte 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 an Soll beim Fund eines Virus bzw. unerwünschten Programms eine Email verschickt werden:
- Geben Sie eine Email-Adresse an.

### Bereich Erweitert

|               |                        |                    |                      |    |
|---------------|------------------------|--------------------|----------------------|----|
| Basis         | <b>Archive Scannen</b> | Maximale Größe     | 1024                 | MB |
| Unerwünschtes |                        | Maximale Rekursion | 20                   |    |
| Erweitert     |                        | Temp. Verzeichnis  |                      |    |
|               |                        | PID Verzeichnis    |                      |    |
|               |                        | Log Datei          | /var/log/avguard.log |    |
|               | System Log             | Priorität          | notice               |    |
|               |                        | Möglichkeit        | user                 |    |
|               | Anzahl der Daemons     |                    | 3                    |    |

Akzeptieren Abbruch

Archive Scannen Hierdurch werden `ArchiveMaxSize` und `ArchiveMaxRecursion` in `avguard.conf` gesetzt.

✓ Optionsfeld **Archive Scannen** im Bereich **Basis** ist aktiviert

Wenn die maximale Größe der zu scannenden Archive (in MB) beschränkt werden soll:

- ▶ Geben Sie den gewünschten Wert ein (in MB).
- ODER –

Wenn es keine Beschränkung geben soll:

- ▶ Wählen Sie **kein Limit**.

Wenn die Rekursionstiefe von verschachtelten Archive beschränkt werden soll:

- ▶ Geben Sie den gewünschten Wert ein.
- ODER –

Wenn rekursive Archive unabhängig von der Rekursionstiefe vollständig entpackt werden sollen:

- ▶ Wählen Sie **kein Limit**.

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 Dämonen Die Anzahl der AntiVir Guard-Dämonen, die gleichzeitig laufen, kann zwischen 0 und 20 eingestellt werden. Der voreingestellte Wert 3 ist sinnvoll für kleinere Standardrechner. Für leistungsfähige Industrie-PC kann eine höhere Anzahl sinnvoll sein.

Wenn der Wert auf **ausschalten** gesetzt wird, wird der AntiVir Guard deaktiviert.

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

- ▶ Wählen Sie die gewünschte Anzahl der Dämonen.

## 7 Service

### 7.1 Support

- Support-Service** Auf unserer Webseite <http://www.antivir.de> erhalten Sie alle Informationen zu unserem umfangreichen Support-Service.
- Die Kompetenz und Erfahrung unserer Entwickler stehen Ihnen hier zur Verfügung. Die Experten der H+BEDV Datentechnik 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.
- Forum** Bevor Sie die Hotline kontaktieren, empfehlen wir einen Besuch in unserem Benutzerforum unter <http://forum.antivir.de>. Möglicherweise sind hier schon Ihre Fragen von anderen Benutzern gestellt und beantwortet worden.
- Email-Support** Support über Email erhalten Sie über <http://www.antivir.de>.

### 7.2 Online-Shop

Sie wollen unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der H+BEDV Datentechnik GmbH können Sie unter <http://www.antivir.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    H+BEDV Datentechnik GmbH  
                  Lindauer Strasse 21  
                  D-88069 Tettnang  
                  Deutschland

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



## 8 Anhang

### 8.1 Glossar

| <b>Begriff</b>                 | <b>Erklärung</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 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 syslog 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                         | <p>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 0190 in Deutschland, 09x0 in Österreich und in der Schweiz und mittelfristig auch in Deutschland).</p> <p>Manchmal werden Dialer bewusst unauffällig eingesetzt, bisweilen in betrügerischer Absicht. Dies kann zu horrenden Telefonrechnungen führen.<br/>AntiVir erkennt Dialer.</p> |
| 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)                                                                                                                                                                                                                                                                                                                                                                                                     |

| <b>Begriff</b>                    | <b>Erklärung</b>                                                                                                                                                                                                                                                                                           |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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).                                                                                |
| PMS (Possible 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 syslog-Dämons wird in /etc/syslog.conf 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.antivir.de/infos/virenkunde.htm>

### 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.





**Programm & Dokumentation**  
**Copyright © 2005**  
**H+BEDV Datentechnik GmbH**  
**Alle Rechte vorbehalten**

**Herausgeber:**  
**H+BEDV Datentechnik GmbH**  
**D-88069 Tettnang, Lindauer Strasse 21**

**Tel.: +49 (0) 7542 / 500 0**  
**Fax: +49 (0) 7542 / 52510**

**Internet: <http://www.antivir.de>**  
**<http://www.hbedv.com>**

**Ausgabe Februar 2005**