



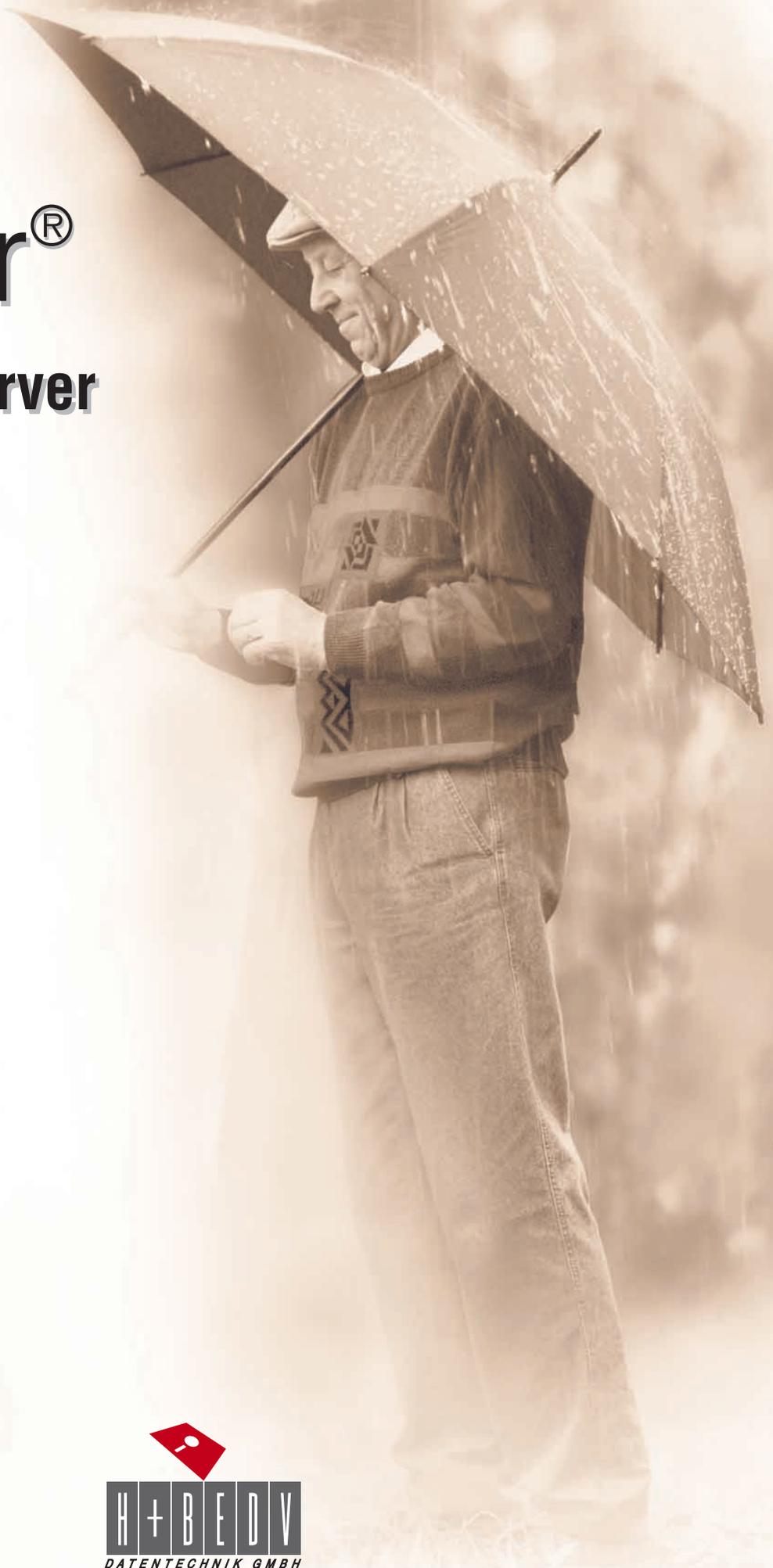
AntiVir®

für Linux Server

Benutzerhandbuch



H+B EDV
DATENTECHNIK GMBH



Inhaltsverzeichnis

1	Über dieses Handbuch	3
1.1	Einleitung	3
1.2	Aufbau des Handbuchs	4
1.3	Zeichen und Symbole	5
2	Produktinformationen	6
2.1	Leistungsumfang	7
2.2	Lizenzierungskonzept	8
2.3	Funktionsweise von AntiVir	9
2.4	Systemvoraussetzungen	10
2.5	Technische Informationen	10
3	Installation	11
3.1	Bereitstellen der Installationsdateien	11
3.2	Lizenzierung	12
3.3	Erstellen des Kernel-Moduls Dazuko	13
3.4	Erstinstallation von AntiVir	15
3.5	Erneute Installation von AntiVir	21
4	Konfiguration	23
4.1	Übersicht	23
4.2	Konfigurationsdateien	24
4.3	Konfigurationsskripte	28
4.4	Konfigurieren der Nachrichten von AntiVir	31
4.5	Konfigurieren des residenten Wächters AntiVir Guard	33
4.6	Konfigurieren regelmäßiger Updates	43
4.7	AntiVir für Linux Server testen	50
5	Bedienung	51
5.1	AntiVir Kommandozeilenscanner im Überblick	51
5.2	AntiVir Kommandozeilenscanner in der Anwendung	56
5.3	AntiVir mit grafischer Oberfläche TkAntiVir	62
5.4	Vorgehen bei Fund eines Virus/unerwünschten Programms	66
6	Service	67
6.1	Support	67
6.2	Kontakt	68
	Anhang	69
	Glossar	69
	Weitere Infoquellen	71
	Goldene Regeln zur Virenvorsorge	72

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 67).

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
1 Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole
2 Produktinformationen	Allgemeine Hinweise zur Software AntiVir, zu Aufbau, Funktionsweise, Systemvoraussetzungen und Lizenzierung
3 Installation	Anleitung zur Installation von AntiVir auf Ihrem System
4 Konfiguration	Anleitung zur optimalen Anpassung von AntiVir auf Ihr System
5 Bedienung	Die Arbeit mit AntiVir, nachdem es installiert wurde; gezielte Suche nach Viren und unerwünschten Programmen; Verhalten beim Auffinden von Viren und unerwünschten Programmen
6 Service	Support und Service von H+BEDV
Anhang	Glossar mit Erläuterungen zu Fachbegriffen und Abkürzungen, Goldene Regeln zur Virenvorsorge

1.3 Zeichen und Symbole

In diesem Handbuch werden folgende Zeichen und Symbole verwendet:

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

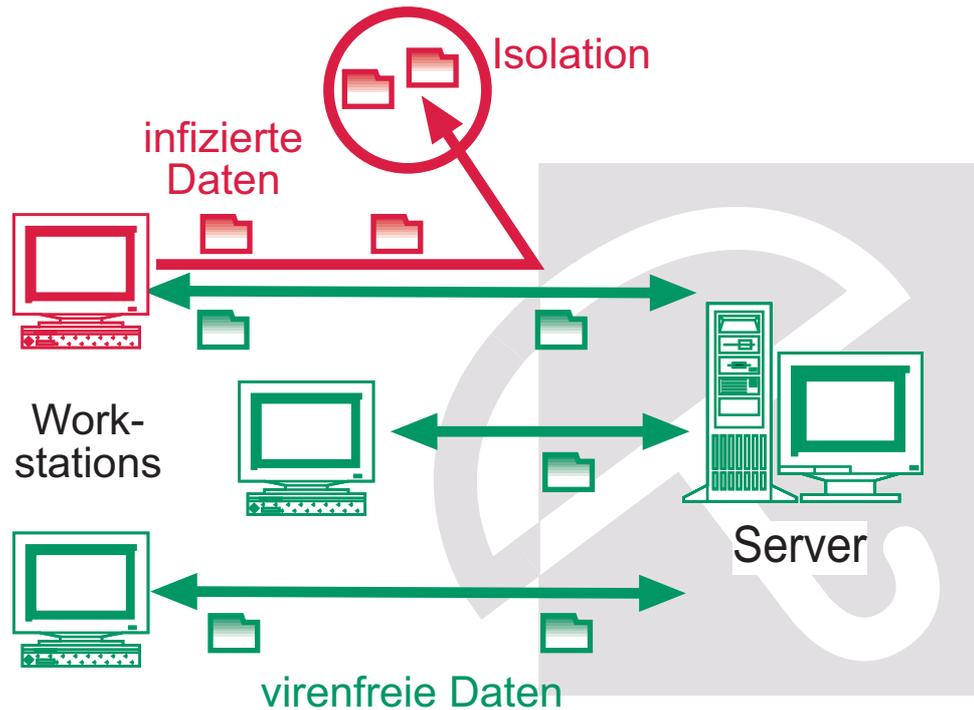
Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

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

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 Linux-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 Linux 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 für Linux Server ist ein umfassendes und flexibles Werkzeug, um der Gefahr vor 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 für Linux Server bietet umfangreiche Konfigurationsmöglichkeiten, damit Sie die Kontrolle über Ihr Netzwerk behalten.

Die wesentlichen Leistungsmerkmale von AntiVir für Linux Server:

- 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 Oberfläche über kostenfreies zusätzliches Modul (siehe [AntiVir mit grafischer Oberfläche TkAntiVir](#) – Seite 62).

2.2 Lizenzierungskonzept

Um AntiVir nutzen zu können, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen von AntiVir an (siehe http://www.anti-vir.de/dateien/anti-vir/handbuch/pdf/eula_anti-vir.pdf).

Sie können die vielfältigen Funktionen von AntiVir im Rahmen folgender Lizenz-Modelle für einen oder mehrere Server nutzen:

- Vollversion
- Fast Update Service (FUSE)
- Komfortpaket

Die Lizenz wird über einen digitalen Lizenzkey in Form der Datei hbedv.key vergeben. Dieser digitale Lizenzkey ist die Schaltzentrale Ihrer persönlichen Lizenz. Er enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Ein digitaler Lizenzkey kann also auch die Lizenz für mehrere Produkte enthalten.

Den digitalen Lizenzkey erhalten Sie von H+BEDV als Datei per Email.

Ohne digitalen Lizenzkey läuft AntiVir als Demoversion.

Demoversion In der Demoversion werden auftretende Viren und unerwünschte Programme gemeldet; es besteht aber keine Möglichkeit, den Zugriff auf betroffene Dateien zu sperren oder sie über AntiVir zu reparieren oder zu verschieben.

Vollversion Zum Leistungsumfang der lizenzierten Vollversion gehören:

- Bereitstellung der AntiVir-Version zum Download aus dem Internet
- Digitaler Lizenzkey zur Freischaltung von der Demoversion auf die Vollversion per Email
- 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 Viren-Definitionsdateien per Internet (für 1 Jahr)
- Kostenfreier Wechsel innerhalb einer Produktpalette und Anrechnung bestehender Lizenzen bei Upgrades/Aufstockung

FUSE FUSE steht für **F**ast-**U**ppdate-**S**ervice. Mit FUSE können Sie den Update-Service über das erste Jahr hinaus für weitere zwölf Monate verlängern.

Zum Leistungsumfang von FUSE gehören:

- Update-Service auf die Programmdateien und die Viren-Definitionsdateien per Internet (für 1 Jahr)
- Ausführliche Installationsanleitung (digital)
- Bereitstellung von PDF-Handbüchern zum Download aus dem Internet
- Newsletter-Service (per Email)
- Kostenfreier Wechsel innerhalb einer Produktpalette und Anrechnung bestehender Lizenzen bei Upgrades/Aufstockung

Komfortpaket Das Komfortpaket enthält zusätzlich zur lizenzierten Vollversion:

- Alle zwei Monate: Kostenlose Lieferung einer bootfähigen CD-ROM mit dem AntiVir Rescue-System und allen aktuellen AntiVir-Programmen
- Umfangreiches Installationshandbuch (gedruckt) bei der Erstauslieferung
- Digitaler Lizenzkey auf Diskette bei der Erstauslieferung
- Newsletter-Service (gedruckt, Versand per Post)

2.3 Funktionsweise von AntiVir

Das Schutzpaket AntiVir für Linux Server besteht aus folgenden Programmteilen:

- [AntiVir Kommandozeilenscanner](#) – Seite 9
- [AntiVir Guard](#) – Seite 10
- [AntiVir Updater](#) – Seite 10

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

AntiVir Updater

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

2.4 Systemvoraussetzungen

AntiVir für Linux 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 2.2.x oder 2.4.x-Kernel

2.5 Technische Informationen

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

Beachten Sie auch die Lizenzinformationen im Installationsverzeichnis unter /legal.

3 Installation

Die aktuelle Version von AntiVir für Linux 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 AntiVir Updater.

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

- [Bereitstellen der Installationsdateien](#) – Seite 11
- [Lizenzierung](#) – Seite 12
- [Erstellen des Kernel-Moduls Dazuko](#) – Seite 13
- [Erstinstallation von AntiVir](#) – Seite 15
- [Erneute Installation von AntiVir](#) – Seite 21

3.1 Bereitstellen der Installationsdateien

Programmdatei aus dem Internet laden

- ▶ Wählen Sie in Ihrem Web-Browser die Adresse <http://www.antivir.de/download/download.htm>
- ▶ Laden Sie die aktuelle Datei, die unter AntiVir für Linux Server abgelegt ist, auf Ihren lokalen Rechner. Zurzeit heißt diese Datei `avlxsrv.tgz`.
- ▶ Legen Sie die Datei auf Ihrem Rechner ab, z.B. unter `/tmp`.

Programmdatei von CD-ROM laden

- ▶ Wählen Sie auf Ihrer CD-ROM den Ordner `/DE/PRODUCTS/LINUX/SERVER`
- ▶ Kopieren Sie die Datei `avlxsrv.tgz` in ein Verzeichnis, z. B. nach `/tmp`.

Programmdatei entpacken

- ▶ Wechseln Sie in das temporäre Verzeichnis:
`cd /tmp`
- ▶ Entpacken Sie die Archivdatei für das AntiVir-Paket:
`tar xzvf avlxsrv.tgz`
 - ↳ Ein Ordner `antivir-x.x.x-server` wird im temporären Verzeichnis angelegt, wobei `x.x.x` für die aktuelle Versionsnummer von AntiVir für Linux Server steht.
- ▶ Wechseln Sie in folgendes Verzeichnis:
`cd /tmp/antivir-x.x.x-server/src`
- ▶ Entpacken Sie die Archivdatei für das Kernel-Modul Dazuko:
`tar xzvf dazuko-x.x.x.tar.gz`
 - ↳ Ein Ordner `dazuko-x.x.x` wird im temporären Verzeichnis angelegt, wobei `x.x.x` für die aktuelle Versionsnummer von Dazuko steht.

3.2 Lizenzierung

Sie müssen AntiVir für Linux Server lizenzieren, um es in vollem Umfang nutzen zu können (siehe [Lizenzierungskonzept](#) – Seite 8). Hierfür benötigen Sie einen digitalen Lizenzkey, der als eigene Datei `hbdev.key` auf einer Diskette oder per Email geliefert wird.

Dieser digitale Lizenzkey enthält Informationen zu Umfang und Dauer der Lizenz. Ohne digitalen Lizenzkey läuft AntiVir für Linux Server ausschließlich als Demoversion mit reduziertem Leistungsumfang.

Lizenz erwerben

- ▶ Kontaktieren Sie uns telefonisch oder per Email (info@antivir.de), um einen gültigen digitalen Lizenzkey für AntiVir zu erhalten.
 - ↳ Sie erhalten einen digitalen Lizenzkey per Email zugesandt.

Digitalen Lizenzkey einspielen

- ▶ Kopieren Sie den digitalen Lizenzkey `hbdev.key` von Diskette oder Email in Ihr Installationsverzeichnis `/tmp/antivir-x.x.x-server`.



Sie können die Installation auch zunächst ohne digitalen Lizenzkey durchführen. AntiVir läuft dann als Demoversion.

Der digitale Lizenzkey kann jederzeit nachträglich in das AntiVir-Programmverzeichnis `/usr/lib/AntiVir` kopiert werden.

3.3 Erstellen des Kernel-Moduls Dazuko



Das Kernel-Modul Dazuko ist nur unter Linux erforderlich.

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



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

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



Im Folgenden wird das Vorgehen so beschrieben, dass Sie auch ohne Expertenkenntnisse zum Ziel kommen. Dennoch sind Kenntnisse in der Kompilierung des Linux-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 Linux-Kernel in `/usr/src/linux` befindet. Falls nicht, installieren Sie ihn nach. Informationen dazu finden Sie in der Dokumentation Ihrer Linux-Distribution.
- ✓ Stellen Sie sicher, dass sich die Programme zur Kompilierung eines Kernels (z. B. `gcc`) auf Ihrem Rechner befinden. Bei einer Linux-Standardinstallation ist dies der Fall. Falls nicht, installieren Sie die benötigten Programmpakete nach. Informationen dazu finden Sie in der Dokumentation Ihrer Linux-Distribution.
- ✓ Ihr Linux-Kernel muss auf dem Quellcode in `/usr/src/linux` basieren. In den meisten Fällen, insbesondere nach einer Neuinstallation von Linux, sollte dies der Fall sein. Absolute Sicherheit hierüber können Sie allerdings nur gewinnen, indem Sie den gesamten Kernel neu kompilieren.



Bei Unsicherheiten über den Stand Ihres Linux-Kernels sollten Sie dennoch die Installation fortführen. Schlimmstenfalls gelingt später die Integration von Dazuko in Ihren Linux-Kernel nicht. Das AntiVir-Installationsskript prüft dies aber und gibt gegebenenfalls eine Meldung aus.

- ▶ Ermitteln Sie Ihre Linux-Version mit dem Befehl **uname**:

```
uname -a
```

↳ Sie erhalten einen Output mit Informationen zum System wie z. B.:

```
Linux mycomputer 2.4.18-4GB #1 Wed Mar 27 13:57:05 UTC  
2002 i586 unknown
```

- ▶ Prüfen Sie, ob im Output **SMP** erscheint. Wenn **SMP** erscheint, haben Sie einen "SMP-Kernel", andernfalls einen "Nicht-SMP-Kernel".
- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie Dazuko entpackt haben, also etwa:

```
cd /tmp/antivir-x.x.x-server/src/dazuko-x.x.x
```

Wenn Sie einen SMP-Kernel haben:

- ▶ Kompilieren Sie Dazuko mit

```
make dazuko-smp
```

Wenn Sie einen Nicht-SMP-Kernel haben:

- ▶ Kompilieren Sie Dazuko mit

```
make dazuko
```

Am Ende erhalten Sie eine Datei `dazuko.o` im temporären Verzeichnis `/tmp/antivir-x.x.x-server/src/dazuko-x.x.x`. Diese Datei wird später vom AntiVir-Installationsskript benötigt.



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

3.4 Erstinstallation von AntiVir

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 AntiVir Updater und des residenten Wächters AntiVir Guard.
- Optional Konfigurieren eines automatischen Starts des AntiVir Updater und des AntiVir Guard beim Systemstart.

Folgende Schritte sind für die Erstinstallation erforderlich:

- [Installation vorbereiten](#) – Seite 15
- Wenn Dazuko noch nicht kompiliert wurde: [AntiVir ohne den AntiVir Guard installieren](#) – Seite 16
- Wenn Dazuko bereits kompiliert wurde: [AntiVir mit dem AntiVir Guard installieren](#) – Seite 18

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-x.x.x-server
```

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 Installationskript 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 bin/antivir-fc 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
installation of command line scanner complete
```

- ↳ Anschließend wird gefragt, ob ein Link in /usr/bin erstellt werden soll:

```
Would you like to create a link in /usr/bin ? [y]
```

- ▶ Bestätigen Sie die Anfrage mit `y` oder `[Enter]`. Sie können dann später AntiVir ohne komplette Pfadangabe aus jedem Verzeichnis heraus starten.

- ↳ Anschließend wird gefragt, ob der AntiVir Updater installiert werden soll:

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



Der AntiVir 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 59

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

Installation
mit Updater

Wenn Sie den AntiVir Updater installieren wollen (empfohlen):

► Geben Sie **Y** ein.

↳ Der AntiVir Updater wird installiert. Anschließend werden Sie gefragt, ob der AntiVir 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 AntiVir 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 2.0.7 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 has been compiled as a kernel module
kernel - Dazuko has been compiled into the Linux kernel
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]**.

Start Konfiguration

Am Schluss haben Sie die Möglichkeit, AntiVir zu konfigurieren:

```
4) 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 13).

► 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 bin/antivir-fc 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
installation of command line scanner complete
```

↳ Anschließend wird gefragt, ob ein Link in `/usr/bin` erstellt werden soll:

```
Would you like to create a link in /usr/bin ? [y]
```

- ▶ Bestätigen Sie die Anfrage mit `y` oder `[Enter]`. Sie können dann später AntiVir ohne komplette Pfadangabe aus jedem Verzeichnis heraus starten.
 - ↳ Anschließend wird gefragt, ob der AntiVir Updater installiert werden soll:

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

i

Der AntiVir 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 59

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

Installation
mit Updater

Wenn Sie den AntiVir Updater installieren wollen (empfohlen):

- ▶ Geben Sie `y` ein und drücken Sie `[Enter]`.
 - ↳ Der AntiVir Updater wird installiert. Anschließend werden Sie gefragt, ob der AntiVir Updater beim Systemstart automatisch gestartet werden soll:

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

Would you like the automatic updater to start automa-
tically? [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 AntiVir 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 has been compiled as a kernel module
kernel - Dazuko has been compiled into the Linux ker-
nel
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-x.x.x-server/src/dazuko-x.x.x/` liegt, geben Sie ein:

```
/tmp/antivir-x.x.x-server/src/dazuko-x.x.x/dazuko.o
```

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

```
testing /tmp/antivir-x.x.x-server/src/dazuko-x.x.x/
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
checking for existing /etc/avguard.conf ... not found
copying conf/avguard.conf to /etc ... 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 Linux-Kernel neu kompilieren. Hinweise hierzu finden Sie unter <http://www.dazuko.org>

Start Konfi-
guration

Am Schluss haben Sie die Möglichkeit, AntiVir zu konfigurieren:

```
4) 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
```

3.5 Erneute Installation von AntiVir

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

AntiVir neu 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-x.x.x-server
```

► Geben Sie ein:

```
./install
```

↳ Das Installationsskript läuft weitgehend ab wie in der Erstinstallation beschrieben (siehe [Erstinstallation von AntiVir](#) – Seite 15).

- ▶ Ändern Sie die entsprechenden Einstellungen während der Installation.

AntiVir ist mit den neuen Einstellungen installiert.

4 Konfiguration

Damit AntiVir für Linux 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 24. Wenn Sie die Konfigurationsskripte verwenden möchten, können Sie diesen Abschnitt überschlagen.
- Erklärungen zum allgemeinen Umgang mit den Konfigurationsskripten erhalten Sie in [Konfigurationsskripte](#) – Seite 28
- Spezifische Konfigurationen von AntiVir werden erläutert in
 - [Konfigurieren der Nachrichten von AntiVir](#) – Seite 31
 - [Konfigurieren des residenten Wächters AntiVir Guard](#) – Seite 33
 - [Konfigurieren regelmäßiger Updates](#) – Seite 43
- Abschließend wird in [AntiVir für Linux Server testen](#) – Seite 50 erklärt, wie Sie prüfen können, ob Sie AntiVir korrekt konfiguriert haben.

4.1 Übersicht

Konfigurationsdateien

Die Konfiguration wird in zwei 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.



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 AntiVir Updater und den AntiVir Guard manuell neu starten, damit die Änderungen wirksam werden.

► Geben Sie dafür ein:

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

Konfigurationsdatei `antivir.conf`

Im Folgenden werden die Einträge in `antivir.conf` in der Reihenfolge ihres Auftretens kurz beschrieben.

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, muss der volle Pfad zur Datei angegeben werden, z. B:

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

AutoUpdate... **Update-Plan:**
Die Software kann mit Hilfe des AntiVir 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 tägliche Updates muss folgende Option aktiviert werden:

```
AutoUpdateDaily
```

Für Updates alle 2 Stunden muss folgende Option aktiviert werden:

```
AutoUpdateEvery2Hours
```

Zeitpunkt für Updates:

Wenn tägliche Updates eingestellt sind, kann 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
```

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 [Authentizität der Updates durch GnuPG sicherstellen](#) – Seite 48. 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.

Konfigurationsdatei `avguard.conf`

Im Folgenden werden die Einträge in `avguard.conf` in der Reihenfolge ihres Auftretens kurz beschrieben.

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 `AccessMask` 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 also 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. 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. Wenn noch nicht vorhanden, wird dieses automatisch angelegt.

Beispiel:

```
MoveConcerningFilesTo /home/quarantine
```

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 35). 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. 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
```

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 Scripte 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 specified. Look them over to make sure they are correct.
number of daemons:                3
scan on:                           close
repair concerning files:          yes
handling of concerning files:    move to /tmp/quarantine
include paths:                     /usr/lib:/usr/bin:/home
exclude paths:                     /home/myhome
scan archives:                     yes
max archive size:                 1073741824 bytes
max archive recursion:           5 levels
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 , 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 configuration? [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 AntiVir Updater aus und fragt, ob der AntiVir Updater gestartet werden soll:

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

- ▶ Geben Sie `y` oder `[Enter]` ein, um den AntiVir Updater zu starten.
 - ↳ Der AntiVir Updater wird gestartet. Wenn der AntiVir 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 Linux-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 Konfigurationskripts 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? [n]
```

- ▶ 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 `[Enter]`, 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 `[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]`.

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-Verzeichnis und das temporäre Verzeichnis von AntiVir MailGate nicht überwachen. Ansonsten blockiert der AntiVir Guard den Zugriff von AntiVir MailGate auf Email-Attachments, die Viren oder unerwünschte Programme enthalten.

Falls die betroffenen Verzeichnisse in Ihren überwachten Verzeichnissen liegen (siehe [Überwachte Verzeichnisse definieren](#) – Seite 33), 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 , 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 Konfigurationskripts 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 eine Datei 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
recommended 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 Konfigurationskripts 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.
- Durch eine Scan beim Ausführen der Datei verhindert man, Viren oder unerwünschte Programme sich durch die Ausführung eines Programms verbreiten.

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

- ▶ 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 everything. 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 Konfigurationskripts mit `[Enter]`.

Das Scannen gepackter Dateien ist konfiguriert.

4.6 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 59.

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

1. Sie verwenden den mitgelieferten AntiVir Updater, den Sie einfach konfigurieren können. Dies ist empfohlen, wenn Sie geringe Linux-Kenntnisse haben und wenig eigene Anpassungen vornehmen möchten.
2. Sie verwenden AntiVir in Verbindung mit dem cron-Dämon. Dies ist empfohlen, wenn Sie vertiefte Linux-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 Linux-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/password? [n]
```

Wenn ein Username und Passwort erforderlich sind:

- ▶ Geben Sie `y` ein.
 - ↳ Anschließend werden Sie nach Username und Passwort gefragt.
- ▶ Geben Sie Username und Passwort ein.
- ▶ Bestätigen Sie alle nachfolgenden Fragen des Konfigurationskripts mit `[Enter]`.

Der Internet-Zugang für Updates ist konfiguriert.

Automatische Updates über den AntiVir Updater konfigurieren

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

```
antivir --update
```



Damit die nachfolgenden Einstellungen wirksam werden können, muss der AntiVir Updater installiert sein. Wenn Sie die Installation wie unter [Erstinstallation von AntiVir](#) – Seite 15 beschrieben vorgenommen haben, ist dies auch der Fall. Ansonsten müssen Sie nochmals das Installationskript laufen lassen, siehe [Erneute Installation von AntiVir](#) – Seite 21.

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 current 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 `[Enter]`.

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

AntiVir Updater manuell starten und anhalten

Wenn Sie den AntiVir Updater starten wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater start
```

Wenn Sie den AntiVir Updater anhalten wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater stop
```

Wenn Sie den aktuellen Status des AntiVir Updater feststellen wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater status
```

AntiVir Updater automatisch starten

Es ist sinnvoll, den AntiVir Updater bei jedem Systemstart automatisch zu starten. Wenn Sie die Installation so vorgenommen haben, wie in [Erstinstallation von AntiVir](#) – Seite 15 beschrieben, ist Ihr System schon entsprechend eingestellt.

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

- ▶ Führen Sie eine [Erneute Installation von AntiVir](#) – Seite 21 mit den entsprechenden Einstellungen durch.

Updates über Cron steuern

Wenn Sie vertiefte Linux-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 Linux-Dokumentation.

Bei der Steuerung der Updates über den Cron-Dämon haben Sie mehr Konfigurationsmöglichkeiten als mit dem AntiVir 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 52

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 Linux 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
```
- ▶ 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-Installationsverzeichnis, also etwa:

```
cd /tmp/antivir-x.x.x-server/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 AntiVir 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.

4.7 AntiVir für Linux 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 eicar2.com
```

 - ↳ 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 26)
- ▶ 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 23 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 Linux-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 51 erhalten Sie einen Überblick über sämtliche Optionen des Kommandozeilenscanners.
- In [AntiVir Kommandozeilenscanner in der Anwendung](#) – Seite 56 werden exemplarische Anwendungen des Kommandozeilenscanners aufgeführt.
- In [AntiVir mit grafischer Oberfläche TkAntiVir](#) – Seite 62 wird beschrieben, wie Sie den AntiVir Kommandozeilenscanner über eine kostenlos erhältliche grafische Oberfläche bedienen können.
- In [Vorgehen bei Fund eines Virus/unerwünschten Programms](#) – Seite 66 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]
```

In den Dateinamen sind auch Wildcards erlaubt. Beispiel:

```
antivir "*.exe"
```

Dieser Aufruf scannt alle Dateien mit der Erweiterung .exe im aktuellen Verzeichnis. Damit die Wildcards nicht von der Linux-Shell fehlinterpretiert werden, sollte man in diesem Fall das Argument *.exe in Anführungszeichen einschließen.

Optionen

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

Option	Funktion
--allfiles	Alle Dateien werden gescannt, nicht nur Programmdateien
-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. Siehe CRC-Datenbank verwenden – Seite 61
-cn	Nur in Verbindung mit -cf verwendbar. Siehe CRC-Datenbank verwenden – Seite 61
-cu	Nur in Verbindung mit -cf verwendbar. Siehe CRC-Datenbank verwenden – Seite 61
-cv	Nur in Verbindung mit -cf verwendbar. Siehe CRC-Datenbank verwenden – Seite 61
-del	Bei einem Fund werden betroffene Dateien gelöscht
-dmcnv	Dokumentenvorlagen werden zu Dokumenten konvertiert
-dmnda	Alle Makros werden gelöscht
-dmdas	Alle Makros eines Dokuments werden gelöscht, wenn eins verdächtig erscheint
-dmDEL	OLE-Dokumente mit verdächtigen Makros werden gelöscht

Option	Funktion
-dmds	Verdächtige Makros werden gelöscht
-dmpack	Dokumentenvorlagen werden komprimiert
-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.
--help	Alle möglichen Optionen werden ausgegeben
--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 den unter <dateiname> angegebenen digitalen Lizenzkey
-lang:DE	AntiVir gibt deutsche Texte aus
-lang:EN	AntiVir gibt englische Texte aus
-noboot	Die Bootsektorprüfung wird abgeschaltet. Hiermit kann bei gezielten Suchläufen Zeit gespart werden, ansonsten wird die Option nicht empfohlen.
-nobreak	Ctrl-C und Ctrl-Break werden deaktiviert. Hierdurch kann verhindert werden, dass ein Nutzer den Scanprozess abbricht.
-nolnk	Symbolische Links werden ignoriert
-nombr	Die Master-Bootsektorprüfung wird abgeschaltet. Hiermit kann bei gezielten 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.

Option	Funktion
-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">- %d: Tag- %m: Monat- %y: Jahr
-ro	Die Logdatei überschreibt die bestehende Logdatei
-rs	Meldungen über Viren und unerwünschte Programme werden einzeilig ausgegeben
-s	Alle Unterverzeichnisse werden durchsucht
--temp=<dir>	AntiVir legt seine temporären Dateien in <dir> ab
--update	AntiVir führt ein Update seiner eigenen Dateien durch, um den Schutz vor Viren und unerwünschten Programmen wieder auf den neuesten Stand zu bringen
-v	Ein Intensiv-Scan wird durchgeführt. AntiVir prüft komplette Dateien. Möglicherweise werden hierbei auch Fehlmeldungen ausgegeben. Diese Option sollte nur im Ausnahmefall gewählt werden, z. B. nach einem Fund.
--version	Die Version von AntiVir wird angezeigt

Option	Funktion
-z	Dateien in gepackten Archiven werden entpackt, gescannt und wieder komprimiert
@<rspdatei>	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 Linux-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
100	AntiVir hat nur den Hilfetext angezeigt
101	Ein Makro wurde in einer Datei gefunden (bei Aufruf von AntiVir mit -dmse)
102	AntiVir startet nicht, weil der Parameter -once 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 antivir.vdf konnte nicht gelesen werden

Exit-Code	Bedeutung
213	Initialisierungsfehler
214	Digitaler Lizenzkey 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
>=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:

<code>--allfiles</code>	Scannt alle Dateien
<code>-s</code>	Scannt alle Unterverzeichnisse
<code>-z</code>	Scannt auch gepackte Dateien
<code>-e -ren</code>	Versucht, betroffene Dateien zu reparieren und benennt irreparable Dateien um

- Geben Sie ein:

```
antivir --allfiles -s -z -e -ren /
```

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 Linux-System DOS-Partitionen vorhanden und gemounted, sollten diese auch geprüft werden.

Hier sind folgende Optionen sinnvoll:

<code>--allfiles</code>	Scannt alle Dateien
<code>-s</code>	Scannt alle Unterverzeichnisse
<code>-e -ren</code>	Versucht, betroffene Dateien zu reparieren und benennt irreparable Dateien um

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

- Geben Sie ein:

```
antivir --allfiles -s -e -ren /var /mnt
```

Betroffene Dateien löschen

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

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

Hier sind folgende Optionen sinnvoll:

<code>--allfiles</code>	Prüft alle Dateien
<code>-del</code>	Löscht betroffene Dateien
<code>-e -del</code>	Versucht, betroffene Dateien zu reparieren und löscht irreparable Dateien



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

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

- Geben Sie ein:

```
antivir --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
```

Verdächtige Makros löschen

AntiVir hat eine so genannte "Makrovirenheuristik". Hiermit können Makros, die virustypische Merkmale aufweisen, ohne dass ein bekannter Virus bzw. ein bekanntes unerwünschtes Programm gefunden wird, als "verdächtig" eingestuft werden. Diese verdächtigen Makros werden in jedem Fall gemeldet.

AntiVir bietet zusätzlich folgende Optionen:

-dmds	Verdächtige Makros werden gelöscht. Möglicherweise bleiben dadurch andere, ebenfalls zum Virus bzw. unerwünschten Programm gehörige Makros im Dokument.
-dmdas	Alle Makros eines Dokuments werden gelöscht, wenn eins verdächtig erscheint. Möglicherweise werden dadurch auch nützliche Makros gelöscht
-dmda	Alle Makros in allen Dokumenten werden gelöscht
-dmdel	OLE-Dokumente mit verdächtigen Makros werden komplett gelöscht. Dies ist die "radikalste" Methode.



Im nachfolgenden Beispiel werden Dateien umgewandelt oder gelöscht. Dabei kann wertvoller Datenbestand verloren gehen.

Beispiel Wenn Sie alle Makros in Dateien mit verdächtigen Makros in /home/myoffice löschen wollen:

► Geben Sie ein:

```
antivir -dmdas /home/myoffice
```

Dokumentenvorlagen konvertieren

Da Makroviren nur Dokumentenvorlagen angreifen können, wandelt ein Makrovirus Dokumente in Dokumentenvorlagen um.

AntiVir kann

- Dokumentenvorlagen wieder in Dokumente zurückführen, nachdem die Makros gelöscht wurden
- Dokumentenvorlagen komprimieren, so dass nicht nur das Makro gelöscht wird, sondern auch sein Name und alle Referenzen. Hierdurch wird verhindert, dass andere Antivirenprogramme noch auf den

Makronamen reagieren und einen Virus bzw. ein unerwünschtes Programm melden, wo keiner/keines mehr ist.

Hierfür bietet AntiVir folgende Optionen:

-dmcnv	Dokumentenvorlagen werden zu Dokumenten konvertiert
-dmda	Alle Makros in allen Dokumenten werden gelöscht
-dmpack	Dokumentenvorlagen werden komprimiert
-dmdas	Alle Makros eines Dokuments werden gelöscht, wenn eins verdächtig erscheint. Möglicherweise werden dadurch auch nützliche Makros gelöscht



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

Beispiele Wenn Sie in einem Verzeichnis `/home/office-XXX` alle Makros löschen und alle Dokumentvorlagen in Dokumente umwandeln wollen:

► Geben Sie ein:

```
antivir -dmda -dmcnv /home/office-XXX
```

Wenn Sie in einem Verzeichnis `/home/office-XXX` alle verdächtigen Makros in den Dokumentvorlagen löschen und zusätzlich die Dokumentvorlagen komprimieren wollen:

► Geben Sie ein:

```
antivir -dmds -dmpack /home/office-XXX
```

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
```



Die volle Pfadangabe zur AntiVir-Binärdatei ist sinnvoll, wenn das Programm als **root** ausgeführt wird. Ansonsten kann es möglicherweise zu einer Warnung kommen, wenn AntiVir irrtümlich `/usr/lib/AntiVir` als Pfad annimmt.

AntiVir über ein Skript aktualisieren

Fortgeschrittene Linux-Nutzer können den AntiVir Kommandozeilen-scanner in ein Skript integrieren und die [Exit-Codes](#) – Seite 55 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 AntiVir mit grafischer Oberfläche TkAntiVir

Für Benutzer, die grafische Oberflächen gewohnt sind, gibt es Unterstützung: TkAntiVir ist ein Skript, mit dem der Benutzer die Parameter von AntiVir mit Hilfe einer grafischen Oberfläche per Mausklick auswählen und an den AntiVir Kommandozeilenscanner übergeben kann.

TkAntiVir unterliegt der GNU General Public License (<http://www.gnu.org>) und steht kostenfrei auf der Homepage des Autors Sebastian Geiges unter http://www.geiges.de/tkantivir/download_dt.htm zur Verfügung. Hier erhalten Sie auch weiterführende Informationen.

TkAntiVir installieren

Die Installation ist abhängig von Ihrer Linux-Version und von der Version von TkAntiVir, die Sie wählen. Weitere Hinweise erhalten Sie unter http://www.sebastian-geiges.de/tkantivir/download_dt.htm. Im Folgenden wird die Installation kurz beispielhaft für die Datei tkav.tgz erklärt:

- ▶ Loggen Sie sich ein als **root**.
- ▶ Legen Sie ein Verzeichnis für die Installationsdateien an, z. B. /tmp/tkav. Legen Sie die heruntergeladene Programmdatei in diesem Ordner ab. Wechseln Sie in diesen Ordner.
- ▶ Entpacken Sie die heruntergeladene Programmdatei:

```
tar xzvf tkav.tgz
```
- ▶ Rufen Sie das Installationsskript auf:

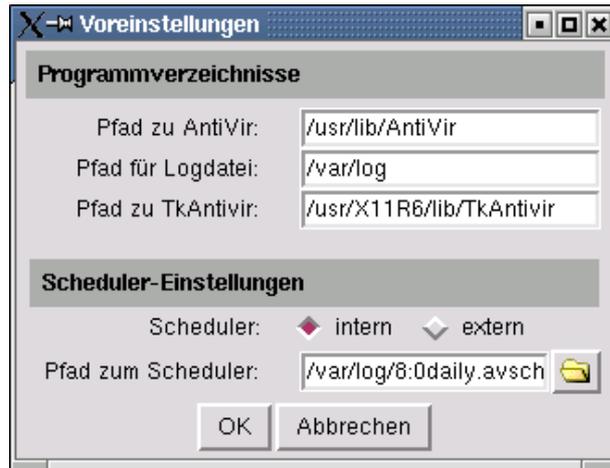
```
./configure
```
- ▶ Geben Sie die Zielpfade für TkAntiVir an:
 - ↳ Die Programmdateien werden kopiert.

TkAntiVir konfigurieren

- ▶ Rufen Sie TkAntiVir auf:

```
TkAntiVir
```

 - ↳ Beim ersten Aufruf erscheint die Meldung, dass TkAntiVir noch konfiguriert werden muss. Anschließend erscheint das Konfigurationsfenster:

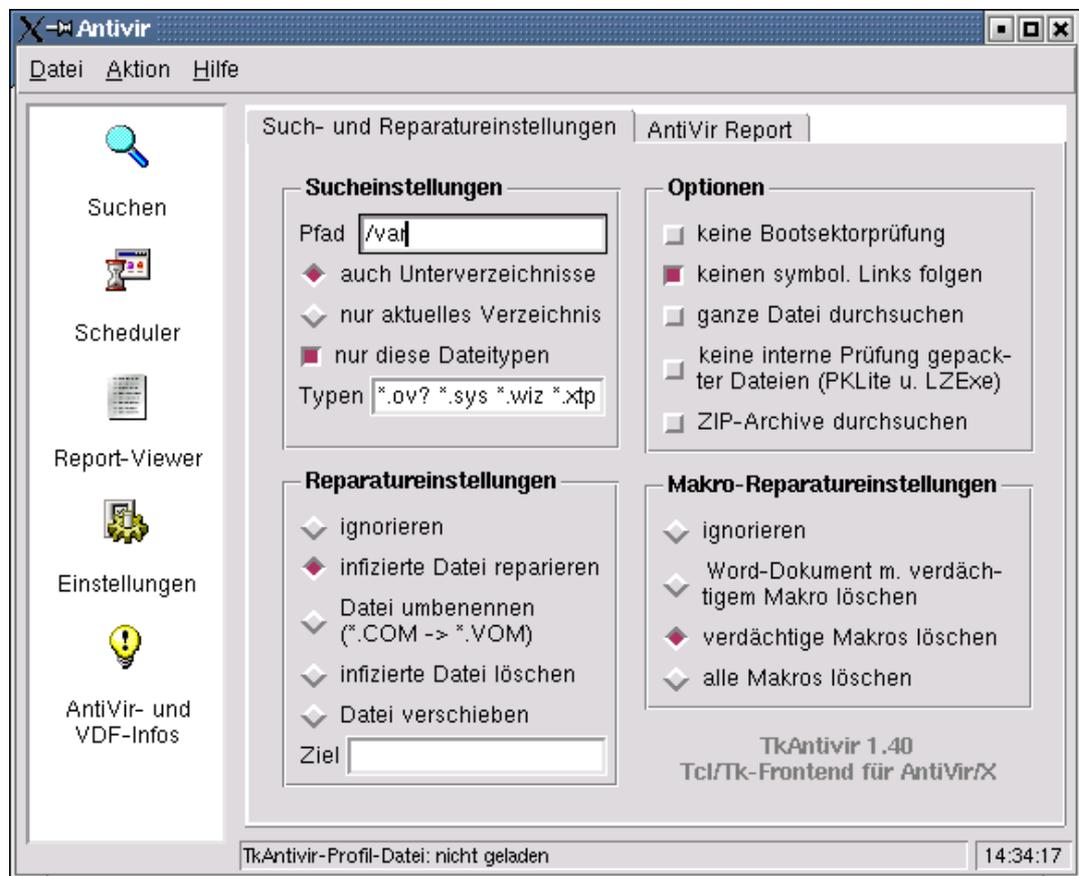


- ▶ Geben Sie hier die korrekten Pfade ein. Der **Pfad zum Scheduler** bleibt zunächst frei.

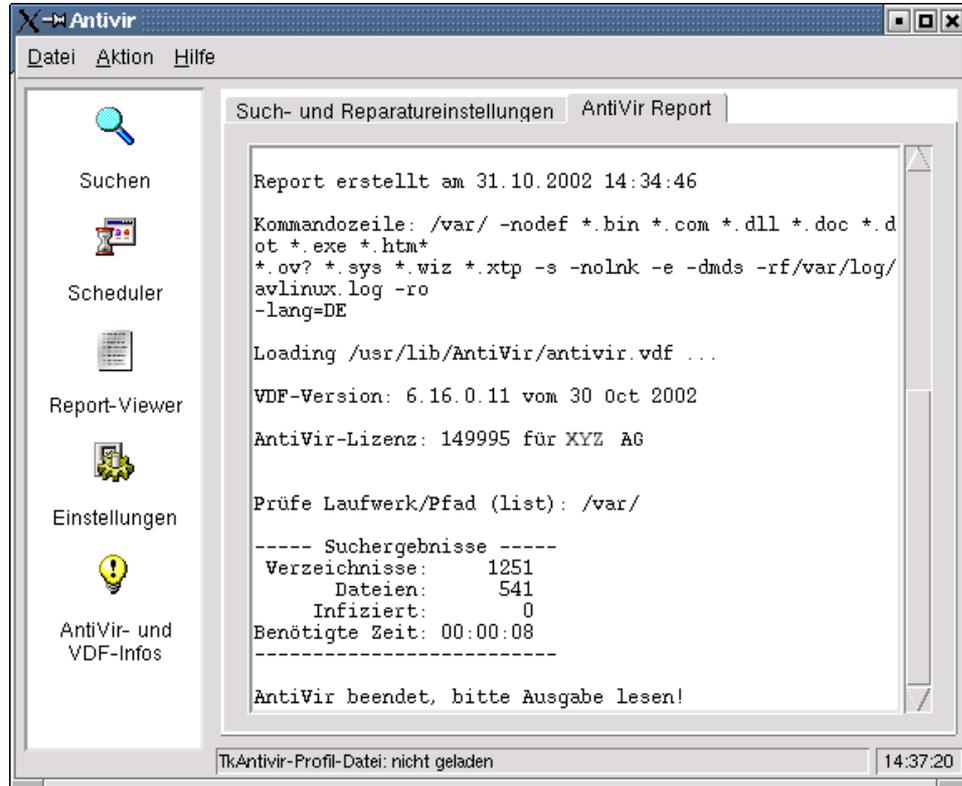
TkAntiVir bedienen

Beim Aufruf von TkAntiVir erscheint das Hauptfenster. Es ist weitgehend selbsterklärend.

- ▶ Wählen Sie die gewünschten Einstellungen für den AntiVir Kommandozeilenscanner über die betreffenden Kontrollkästchen und Optionen an. Beispiel:



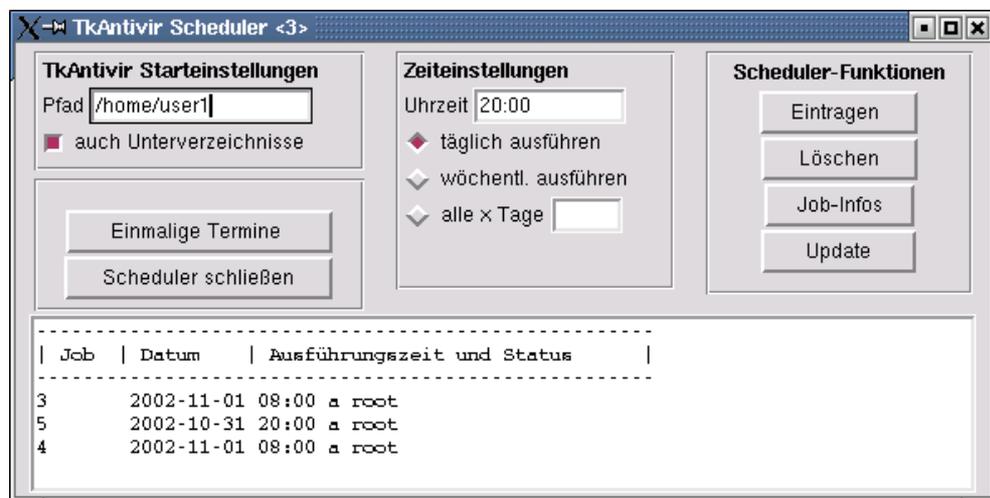
- ▶ Klicken Sie auf das Symbol **Suchen**, um den Suchlauf zu starten.
 - ↳ Der AntiVir Kommandozeilenscanner wird mit den gewählten Einstellungen aufgerufen. Das Ergebnis des Suchlaufs wird in der Logdatei ausgegeben:



Suchläufe planen

TkAntiVir kann über einen Planer Jobs erstellen, so dass der AntiVir Kommandozeilenscanner zu definierten Zeiten (einmalig oder regelmäßig wiederkehrend) aufgerufen wird.

- ▶ Klicken Sie das Symbol **Scheduler**, um den Planer zu starten.
 - ↳ Das Planer-Fenster erscheint:



- ▶ Definieren Sie einen Job. Tragen Sie dafür die gewünschten Einstellungen ein:
 - unter **TkAntiVir Starteinstellungen** den Pfad ein, der gescannt werden soll
 - unter **Zeiteinstellungen** die gewünschten Zeiten, zu denen der Scan durchgeführt werden soll.
Mit der Schaltfläche **Wiederkehrende Termine/Einmalige Termine** schalten Sie zwischen regelmäßigen und einmaligen Jobs um.
- ▶ Übernehmen Sie die Einstellungen über **Eintragen** in die Jobliste.
- ▶ Definieren Sie, wenn gewünscht, weitere Jobs und übertragen Sie sie in die Jobliste.

Wenn Sie alle Jobs definiert haben:

- ▶ Schließen Sie den Planer über **Scheduler schließen**.

Der AntiVir Kommandozeilenscanner wird jetzt zu den definierten Zeiten aufgerufen.

5.4 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 (gzip, WinZIP, PKZip, Arj) im Anhang einer Email an virus@antivir.de.



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

6 Service

6.1 Support

Support-Service Auf unserer Webseite www.antivir.de/support/suport.htm erhalten Sie alle nötigen 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/support/quick-mail.htm>.

6.2 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>.

Anhang

Glossar

Begriff	Erklärung
Backdoor-Steuerprogramme (BDC)	Um Daten zu stehlen oder Rechner zu manipulieren, wird ein Backdoor-Steuerprogramm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder 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 Linux. Im Schnitt laufen einige Dutzend Dämonen auf dem Rechner. Diese Prozesse werden beim Hochfahren des Rechners gestartet
Demoversion	Ohne gültigen digitalen Lizenzkey läuft AntiVir für Linux 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. 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 unbekanntem Makroviren. Hierbei wird das Makro beim Auffinden von virustypischen Funktionen als "verdächtig" gemeldet.

Begriff	Erklärung
Kernel	Innerster Teil des Betriebssystems mit elementaren Systemfunktionen (Speicherverwaltung, Prozessverwaltung)
Logdatei	auch: Reportdatei, Protokolldatei. Datei, in die Meldungen von Programmen geschrieben wird
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)	"Mögliche 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 Linux 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.
Virendefinitionsdatei	siehe VDF

Weitere Infoquellen

Weitere Informationen zu verschiedenen Viren, Würmern, Makroviren und weiteren unerwünschten Programmen sind erhältlich unter

<http://www.antivir.de/infos/virenkunde.htm>

Goldene Regeln zur Virenvorsorge

- ▶ Erstellen Sie Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkservers 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 © 1991-2003
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 August 2003