



**AntiVir®**

**Milter  
für Sendmail**

# Benutzerhandbuch



**H+BEDV**  
DATENTECHNIK GMBH



# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>1</b>
1.1	Zielgruppen	1
1.2	Funktionalität von AntiVir Milter für Linux	1
<b>2</b>	<b>Integration von AntiVir Milter in sendmail</b>	<b>2</b>
2.1	Voraussetzung	2
2.2	Integration	2
<b>3</b>	<b>Installation von AntiVir Milter</b>	<b>4</b>
3.1	Voraussetzung	4
3.2	Installation	4
<b>4</b>	<b>Konfiguration von AntiVir Milter</b>	<b>7</b>
4.1	Arbeitsweise von AntiVir Milter	7
4.2	Einstellung der Konfiguration in avmilter.conf	7
<b>5</b>	<b>Konfiguration automatischer Updates</b>	<b>15</b>
5.1	Einstellungen in antivir.conf	15
5.2	AntiVir PGP Public-Key - antivir.gpg	16
<b>6</b>	<b>Vorlagen für Meldungen</b>	<b>18</b>



# 1 Einführung

## 1.1 Zielgruppen

Dieses Benutzerhandbuch richtet sich an alle Anwender des AntiVir Milter. Es enthält Informationen für den technisch versierten Laien bis zum Administrator. Grundkenntnisse in Linux werden in jedem Fall vorausgesetzt.

## 1.2 Funktionalität von AntiVir Milter für Linux

AntiVir Milter ist ein PlugIn für sendmail ab Version 8.11 und kommuniziert über die libmilter-Schnittstelle von sendmail.

AntiVir Milter überprüft alle ein- und ausgehenden Emails. Infizierte Emails werden nicht weitergeleitet. Über syslog wird eine Statusmeldung ausgegeben. Absender, Empfänger und Administrator können über Infektionen benachrichtigt werden.

Funktionen:

- Alle Funktionen von sendmail sind weiterhin verfügbar.  
Beispiel: SMTP Authentication, Anti-relaying und Anti-spam
- Einfache Installation und Integration in sendmail
- Stündliches oder tägliches Update der Scan Engine und der Virensignatur-Datei über das Internet
- Überprüfen von ein- und ausgehenden Emails
- Zuverlässige Erkennung von Viren und unerwünschten Programmen in Echtzeit
- Konfigurierbare Reaktion auf einen Fund von Viren und unerwünschten Programmen
- Isolation von infizierten und verdächtigen Dateien in einem Quarantäne-Verzeichnis
- Log-Datei als Protokoll über Email-Verkehr nutzbar
- Sofort-Aktivierung bei neuer Virendefinitionsdatei (.vdf) aus unserem Hause
- Heuristische Makroviren-Erkennung
- Konfigurierbare Templates für eigene Warnmeldungen
- Scannen von Archiven (Anzahl der unterstützten Archiv-Formate wird mit `antivir --version` angezeigt)

## 2 Integration von AntiVir Militer in sendmail

### 2.1 Voraussetzung

Voraussetzung ist sendmail in einer Version ab 8.11 mit libmilter-Schnittstelle.

Wenn dies nicht der Fall ist:

- ⇒ README-Datei im Verzeichnis libmilter im sendmail-Paket lesen (<http://www.sendmail.org>).
- ⇒ Neue Version von sendmail mit libmilter-Schnittstelle kompilieren.

### 2.2 Integration

Anschließend kann AntiVir Militer auf zwei Arten in die Konfigurationsdatei von sendmail, sendmail.cf, eingefügt werden:

- Direkte Bearbeitung von sendmail.cf
- oder
- Generieren von sendmail.cf

#### 2.2.1 sendmail.cf **direkt bearbeiten**

- ⇒ In die Konfigurationsdatei von sendmail, sendmail.cf, die folgenden beiden Zeilen eintragen:

```
Xavmilter, S=inet:3333@localhost, F=R, T=S:10m;R:10m;E:10m
O InputMailFilters=avmilter
```

#### 2.2.2 sendmail.cf **generieren**

- ⇒ In die Datei sendmail.mc die entsprechenden Zeilen eintragen:

bei sendmail 8.11.x:

```
define(`_FFR_MILTER', `true')
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost, F=R,
T=S:10m;R:10m;E:10m')
```

bei sendmail 8.12.x:

```
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost, F=R,
T=S:10m;R:10m;E:10m')
```

- ⇒ Datei sendmail.cf generieren.

Beispiel:

```
m4 sendmail.mc > /etc/mail/sendmail.cf
```

### 2.2.3 Zusatzinformationen

Bei der Konfiguration von sendmail unterstützen wir Sie nur bei Problemen, die direkt mit AntiVir Milter zusammenhängen.

Weitere Informationen finden Sie bei <http://www.sendmail.org>.

Informationen zur libmilter-Schnittstelle finden Sie bei <http://www.milter.org>.

## 3 Installation von AntiVir Milter

### 3.1 Voraussetzung

Voraussetzung ist sendmail in einer Version ab 8.11 mit libmilter-Schnittstelle (siehe Abschnitt 2.1).

### 3.2 Installation

#### 3.2.1 AntiVir Programmpaket wählen

Der Name des AntiVir-Programmpakets hängt vom Betriebssystem ab:

- Free-BSD: avfbmlt.tgz
- Open-BSD: avobmlt.tgz
- Linux: avlxmlt.tgz

Im Folgenden beschreiben wir die Installation für das Betriebssystem Linux.

#### 3.2.2 Dateien entpacken

⇒ Datei avlxmlt.tgz entpacken.

```
tar xzvf avlxmlt.tgz
```

Das Unterverzeichnis antivir-milter-x.x.x wird angelegt (x.x.x steht für die aktuelle Versionsnummer).

⇒ In das Unterverzeichnis antivir-milter-x.x.x wechseln:

```
cd antivir-milter-x.x.x
```

#### 3.2.3 Verzeichnisse anlegen und Dateien kopieren

⇒ Verzeichnis /usr/lib/AntiVir/ anlegen. Datei vdf/antivir.vdf in Verzeichnis /usr/lib/AntiVir/ kopieren. Dabei Groß- und Kleinschreibung des Worts „AntiVir“ beachten:

```
mkdir /usr/lib/AntiVir  
cp vdf/antivir.vdf /usr/lib/AntiVir/
```

⇒ User und Group auf uucp ändern:

```
chown uucp:uucp /usr/lib/AntiVir  
chown uucp:uucp /usr/lib/AntiVir/antivir.vdf
```

- ⇒ Scan-Engine bin/antivir in Verzeichnis /usr/lib/AntiVir kopieren. User und Groups zu uucp ändern:

```
cp bin/antivir /usr/lib/AntiVir
chown uucp:uucp /usr/lib/AntiVir/antivir
```

- ⇒ Dateien avmilter.conf und antivir.conf in Verzeichnis /etc kopieren:

```
cp etc/avmilter.conf /etc/
cp etc/antivir.conf /etc/
```

- ⇒ Programmdatei bin/avmilter in Verzeichnis /usr/sbin/ kopieren:

```
cp bin/avmilter /usr/sbin/
```

- ⇒ Spool-Verzeichnis anlegen (voreingestellt: /var/spool/avmilter). Dieses Verzeichnis darf nur für uucp oder den User, der in /etc/avmilter.conf spezifiziert ist, zugänglich sein:

```
mkdir /var/spool/avmilter
cd /var/spool/avmilter/
mkdir incoming
mkdir outgoing
mkdir rejected
chown -R uucp:uucp /var/spool/avmilter
chmod -R 700 /var/spool/avmilter
```

### 3.2.4 Lizenz-Datei kopieren

Wenn Sie eine Lizenz für den kommerziellen oder privaten Gebrauch besitzen:

- ⇒ Lizenz-Datei hbedv.key in Verzeichnis /usr/lib/AntiVir/avmilter.key kopieren:

```
cp hbedv.key /usr/lib/AntiVir/avmilter.key
chown uucp:uucp /usr/lib/AntiVir/avmilter.key
chmod 440 /usr/lib/AntiVir/avmilter.key
```

Ohne digitalen Lizenzkey läuft AntiVir Milter als Demoversion. Dabei wird der Eintrag in der Betreff-Zeile jeder Email um folgenden Hinweis ergänzt:

- Checked by AntiVir DEMO version -

### 3.2.5 AntiVir Milter in sendmail integrieren

Konfigurationsdatei sendmail.cf editieren (siehe Kapitel 2).

### 3.2.6 Programme starten

- ⇒ AntiVir Milter starten:

```
/usr/sbin/avmilter -p inet:3333@localhost
```

- ⇒ sendmail neu starten (bei SuSE):

```
rcsendmail restart
```

oder

```
killall -HUP sendmail
```

### 3.2.7 Update automatisieren

Die regelmäßige Ausführung von Updates wird über den Cron-Dämon gesteuert.

- ⇒ Entsprechenden Eintrag in der Datei `/etc/crontab` vornehmen.

**Beispiel:** Für ein stündliches Update (z. B. um 23:00 Uhr) folgende Zeile einfügen:

```
23 * * * * root /usr/lib/AntiVir/antivir --update -q
```

- ⇒ Bei Verwendung eines Proxy-Servers: Server-Name und -Anschluss in der Datei `/etc/antivir.conf` eintragen (siehe Kapitel 5.1).

- ⇒ Starten Sie den Update-Vorgang, um die Update-Einstellungen zu testen:

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

Bei erfolgreicher Ausführung liegt in den Log-Dateien `/var/log/mail`, `/var/log/maillog` oder `/var/log/mail.log` eine Nachricht von AntiVir Milter mit der Scan-Engine-Version und VDF-Version.

### 3.2.8 Zugriffsrechte kontrollieren

Wenn Sie die User- und Group-Parameter in `avmilter.conf` ändern (siehe Abschnitt 1):

- ⇒ Sicherstellen, dass die folgenden Dateien die gleichen Zugangsrechte haben:

```
/usr/lib/AntiVir/antivir  
/usr/lib/AntiVir/antivir.vdf  
/usr/lib/AntiVir/avmilter.key
```

- ⇒ Sicherstellen, dass die folgenden Verzeichnisse die gleichen Zugangsrechte haben und für die user und group, die in `avmilter.conf` definiert sind, zugänglich sind:

```
/usr/lib/AntiVir/  
/var/spool/avmilter/  
/var/spool/avmilter/incoming/  
/var/spool/avmilter/outgoing/  
/var/spool/avmilter/rejected/
```

## 4 Konfiguration von AntiVir Milter

### 4.1 Arbeitsweise von AntiVir Milter

AntiVir Milter sorgt dafür, dass eine infizierte Email gesondert abgelegt wird („Quarantäne“) und zusätzlich, je nach Konfiguration, das Auftreten des Virus oder des unerwünschten Programms an den Benutzer gemeldet wird. Diese Arbeitsweise ist über die Datei `avmilter.conf` einstellbar.

AntiVir Milter vergibt für jede Email eine interne Message-ID.

Im Verzeichnis `incoming` werden zunächst zwei Dateien abgelegt. Dieses Verzeichnis liegt in dem Verzeichnis, das in `SpoolDir` angegeben wurde (Standardeinstellung: `/var/spool/avmilter`):

- *df-Message-ID*: Datei, die die Email enthält
- *qf-Message-ID*: Kontrolldatei, die Meta-Informationen zur Email enthält und anzeigt, dass die Email für die Prüfung auf Viren und unerwünschte Programme bereitliegt.

Wenn AntiVir Milter einen Virus oder ein unerwünschtes Programm findet, werden diese Dateien in das Verzeichnis `rejected` verschoben. Dieses Verzeichnis liegt in dem Verzeichnis, das in `SpoolDir` angegeben wurde (Standardeinstellung: `/var/spool/avmilter`). Dabei wird die Kontrolldatei *qf-Message-ID* umbenannt nach:

- *vf-Message-ID* (wenn die Email einen Virus oder ein unerwünschtes Programm enthält)
- *mf-Message-ID* (wenn bei der Email ein MIME-Problem aufgetreten ist).

Im Falle einer Infektion liegen im entsprechenden Verzeichnis (Standardeinstellung: `/var/spool/avmilter/rejected/`) also schließlich:

- *df-Message-ID*
- *vf-Message-ID* oder *mf-Message-ID*

Auf diese Dateien können externe Programme oder Scripte zugreifen, z. B. indem die `ExternalProgram`-Anweisung in der Datei `avmilter.conf` verwendet wird (siehe Abschnitt 4.2).

### 4.2 Einstellung der Konfiguration in `avmilter.conf`

Die Datei `avmilter.conf` enthält einstellbare Parameter zur Arbeitsweise von AntiVir Milter. Zeilen mit `#` am Anfang sind Kommentare oder auskommentierte Befehle. Wenn Parameter nicht spezifiziert sind, werden die Standardeinstellungen der folgenden Liste verwendet.

## User, Group

AntiVir Milter startet unter dem folgenden Besitzer (User) und Gruppe (Group):

```
User                uucp
Group               uucp
```

Wenn diese Einstellungen geändert werden, müssen die Zugriffsrechte auf den betroffenen Verzeichnissen und Dateien nachgezogen werden (siehe Abschnitt 3.2.8).

## Postmaster

Empfänger von Fehlermeldungen und Warnmeldungen über Viren und unerwünschte Programme:

```
Postmaster          postmaster
```

## MyHostName

FQDN (Fully Qualified Domain Name) des lokalen Hosts.

Wenn dies in der Konfigurationsdatei auskommentiert wurde, ist die Standard-einstellung der von `gethostname(2)` zurückgegebene Hostname. Andernfalls ist `localhost` voreingestellt:

```
MyHostName          localhost
```

## SpoolDir

Spool-Verzeichnis von AntiVir Milter. In den Unterverzeichnissen `incoming`, `rejected` und `outgoing` werden Emails während des Prozessablaufs abgelegt (siehe Abschnitt 4.1).

User:Group (wie oben definiert) muss User des Verzeichnisses `SpoolDir` sein und es darf nur für diesen User zugänglich sein (`mode = 0700`):

```
SpoolDir            /var/spool/avmilter
```

## AntiVirDir

Verzeichnis mit dem AntiVir Hauptprogramm, der Virusdefinitionsdatei `antivir.vdf` und dem Lizenzschlüssel:

```
AntiVirDir          /usr/lib/AntiVir
```

## TemporaryDir

In diesem Verzeichnis liegen die temporären Dateien (z. B. Dateianhänge, die auf Viren und unerwünschte Programme untersucht werden). Für ungepackte Anhänge wird entsprechend ausreichender Speicherplatz benötigt.

```
TemporaryDir        /var/tmp
```

oder

```
TemporaryDir        /tmp
```

## LogFile

Die Angabe muss den vollständigen Pfad zur Log-Datei enthalten. Neben den Einträgen in dieser Log-Datei werden auch Einträge an den syslog gesendet.

Wenn LogFile auf NO gesetzt ist, wird keine eigene Log-Datei verwendet. Es werden aber Einträge an den syslog gesendet.

```
LogFile /var/log/avmilter.log
```

oder

```
LogFile NO
```

## MinFreeBlocks

AntiVir Milter blockt eingehende Verbindungen ab, wenn weniger freie Blöcke als der eingestellte Wert (also zu wenig freier Speicher) im File-System des Spool-Verzeichnisses vorhanden sind.

```
MinFreeBlocks 100
```

## ForwardTo

Definiert die ausführbare Datei und die Parameter für den Aufruf von Sendmail:

```
ForwardTo /usr/lib/sendmail -oem -oi
```

## MaxNestingLevel

Definiert die maximale Schachtelungstiefe (Rekursionstiefe) von MIME Emails:

```
MaxNestingLevel 20
```

## MaxAttachments

Definiert die maximale Anzahl von Anhängen, die für eine einzelne MIME Email zugelassen sind:

```
MaxAttachments 100
```

## BlockSuspiciousMime

Blockiert die Zustellung „verdächtiger“ MIME Emails. Eine MIME Email wird als „verdächtig“ eingestuft, wenn die maximale Rekursionstiefe oder die maximale Zahl von Anhängen erreicht ist:

```
BlockSuspiciousMime NO
```

## BlockFragmentedMessage

Blockiert Emails, die beschädigt zugestellt werden:

(Weitere Informationen siehe „Message Fragmentation and Reassembly“, RFC 2046, <http://www.fags.org/rfcs/rfc2046.html>, Abschnitt 5.2.2.1):

```
BlockFragmentedMessage NO
```

**VirusAlertToRcpt**

Sendet Warnmeldungen über Viren und unerwünschte Programme an den/die Empfänger:

`VirusAlertToRcpt` NO

**VirusAlertToSender**

Sendet Warnmeldungen über Viren und unerwünschte Programme an den Absender:

`VirusAlertToSender` NO

**VirusAlertToPostmaster**

Sendet Warnmeldungen über Viren bzw. unerwünschte Programme an den Postmaster (nur in der kommerziellen Version):

`VirusAlertToPostmaster` YES

**VirusAlertsUser**

Benutzername oder Email-Adresse des Absenders der Warnmeldungen (wenn ein Virus oder ein unerwünschtes Programm in der Email gefunden wurde):

`VirusAlertsUser` AntiVir

oder

`VirusAlertsUser` AntiVir@mailserver.mydomain.tld

**RejectVirusMail**

Wenn RejectVirusMail auf YES gesetzt ist, wird eine Email, die einen Virus oder ein unerwünschtes Programm enthält, auf SMTP-Ebene blockiert. Der Absender erhält die Meldung „557 Alert found in mail“.

Wenn RejectVirusMail auf NO gesetzt ist, wird die Email angenommen und in das Quarantäne-Verzeichnis verschoben:

`RejectVirusMail` NO

**ScanInArchive**

Wenn ScanInArchive auf NO gesetzt ist, werden Archive nicht auf Viren und unerwünschte Programme durchsucht.

Wenn ScanInArchive auf YES gesetzt ist, werden alle Dateien in Archiven entpackt und durchsucht, abhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio.

`ScanInArchive` YES

### ArchiveMaxSize (alt: MaxFileSizeInArchive)

Wenn ArchiveMaxSize auf 0 gesetzt ist, werden alle Dateien in Archiven unabhängig von ihrer Größe entpackt.

Wenn ArchiveMaxSize auf einen Wert > 0 gesetzt ist, werden nur die Dateien mit einer entpackten Größe bis zu diesem Wert (in Bytes) entpackt.

Die alte Schreibweise wird derzeit noch akzeptiert, in künftigen Versionen jedoch nicht mehr.

```
ArchiveMaxSize          0
```

### ArchiveMaxRecursion (alt: MaxRecursionDepthInArchive)

Wenn ArchiveMaxRecursion auf 0 gesetzt ist, werden rekursive (verschachtelte) Archive unabhängig von der Rekursionstiefe vollständig entpackt.

Wenn ArchiveMaxRecursion auf einen Wert > 0 gesetzt ist, werden rekursive Archive nur bis zu der Rekursionstiefe, die diesem Wert entspricht, entpackt.

Die alte Schreibweise wird derzeit noch akzeptiert, in künftigen Versionen jedoch nicht mehr.

```
ArchiveMaxRecursion     5
```

### ArchiveMaxRatio

ArchiveMaxRatio blockiert so genannte „Mailbomben“ mit einer sehr hohen Kompressionsdichte.

Der Wert 0 schaltet diese Option aus. Diese Einstellung wird **nicht** empfohlen.

```
ArchiveMaxRatio         150
```

### MaxRecipientsPerMessage

Die Angabe legt die maximale Zahl der Empfänger pro Email fest. Der Wert 0 schaltet diese Option aus.

```
MaxRecipientsPerMessage 100
```

### BlockSuspiciousArchive

Wenn BlockSuspiciousArchive auf YES gesetzt ist, kann die Zustellung von Emails gesperrt werden – abhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio.

Wenn BlockSuspiciousArchive auf NO gesetzt ist, werden Emails unabhängig von den Einstellungen in ArchiveMaxSize, ArchiveMaxRecursion und ArchiveMaxRatio zugestellt:

```
BlockSuspiciousArchive  NO
```

### BlockEncryptedArchive

Wenn BlockEncryptedArchive auf **YES** gesetzt ist, wird die Zustellung von Emails gesperrt, wenn sie verschlüsselte Dateien in einem Archiv enthalten.

Wenn BlockEncryptedArchive auf **NO** gesetzt ist, werden Emails auch zugestellt, wenn Sie verschlüsselte Dateien in einem Archiv enthalten:

BlockEncryptedArchive	NO
-----------------------	----

### AddXHeader

Wenn AddXHeader auf **YES** gesetzt ist, werden Informationen zum Scan-Status dem Header der untersuchten Email hinzugefügt, z. B.: „X-AntiVirus: Checked by ...“ (nur in der kommerziellen Version):

AddXHeader	YES
------------	-----

### ModifySubject

Fügt dem Betreff einer Email die Zeichenfolge „- Checked by AntiVir -“ an:

ModifySubject	NO
---------------	----

### ScanTimeout

Definiert die maximale Dauer des Email-Scans in Sekunden:

ScanTimeout	300
-------------	-----

### ExternalProgram

Ruft ein externes Programm oder ein Skript auf, wenn ein Virus oder ein unerwünschtes Programm gefunden wurde. Der Parameter ist die ID der zurückgewiesenen Email (siehe Abschnitt 4.1):

ExternalProgram	/dir/my_own_script
-----------------	--------------------

### AddPrecedenceHeader

Diese Option ist nur mit einer Lizenz für die kommerzielle Nutzung verfügbar. Wenn **YES** eingestellt ist, erhält die bei einem Virenfund versandte Email den Vermerk „Precedence: junk“. Programme, die auf eingegangene Emails automatisch antworten (z. B.: vacation), reagieren dann nicht auf diese Benachrichtigungs-Email. Der Eintrag **YES** oder **NO** kann durch einen eigenen Text ersetzt werden.

AddPrecedenceHeader	YES
---------------------	-----

## AddressFilter

Mit dieser Option wird der Adressfilter aktiviert/deaktiviert. Standardeinstellung ist `NO`, d. h., dass bei der Standardinstallation kein Adressfilter verwendet wird.

```
AddressFilter          YES
```

Um den Adressfilter nutzen zu können, müssen folgende Dateien vorhanden sein:

```
/etc/avmilter.ignore
```

und

```
/etc/avmilter.scan
```

Diese Dateien enthalten zeilenweise Email-Adressen und optional die Flags `S/s` (Senderadresse) und/oder `R/r` (Empfängeradresse). Die angegebenen Email-Adressen werden nur über das SMTP-Protokoll (MAIL FROM und RCPT TO) geprüft. Die Email-Adressen in den Email-Headern werden nicht beachtet.

Die Listen werden auf Übereinstimmung geprüft. Zuerst wird die Liste geprüft, die an erster Stelle im FilterTableOrder steht. Sobald eine Übereinstimmung vorliegt, wird die weitere Prüfung der Listen abgebrochen und die konfigurierte Aktion ausgeführt.

Je nach Ergebnis werden folgende Aktionen ausgelöst:

- Liegt keine Übereinstimmung mit der ersten Liste vor, wird die nächste Liste geprüft.
- Liegt auch hier keine Übereinstimmung vor, wird die Email gescannt.
- Liegt eine Übereinstimmung mit der ignore-Liste vor, wird die Email nicht gescannt.
- Liegt eine Übereinstimmung mit der scan-Liste vor, wird die Email gescannt.

Die Email-Adressen müssen Perl-kompatible reguläre Ausdrücke sein, z. B.:

```
/abc/
/^abc/
/xyz/i
/^abc@def\.tld/
```

Beispiel:

`/etc/avmilter.ignore` enthält folgende Zeilen:

```
/^jemand@irgendwo\.tld$/ SR
/^virus@firma/ R
/^abc@def.*\.tld/i
```

Ist die Adresse des Senders oder Empfängers `jemand@irgendwo.tld`, wird die Email nicht gescannt.

Ist die Adresse des Empfängers `virus@firma*`, wird die Email nicht gescannt. Die Angabe des Flags `R` ist in diesem Fall optional: `/^virus@firma/` `R` ist gleichbedeutend mit `/^virus@firma/`.

Beim Starten von AntiVir Milter wird im maillog angegeben, ob der Adressfilter aktiv ist oder nicht:

```
addressfilter is active
table order is: ignore,scan
```

oder

```
addressfilter is not active
```

### FilterTableOrder

Die Option ist nur bei aktiviertem Adressfilter (`AddressFilter YES`) von Bedeutung. Mögliche Parameter sind:

```
scan,ignore
```

oder

```
ignore,scan
```

### UseProxy

Scans werden mit der Proxy-Option in SAVAPI effektiver ausgeführt, wenn sie einen festgelegten Pool an AV-Scannern verwenden. Da dieser Pool den Durchsatz erhöht, muss die Größe des Pools sehr genau bestimmt werden: Zu viele Scanner verbrauchen zu viel Ressourcen, ohne die Leistung zu steigern, zu wenige Scanner führen dazu, dass die SAVAPI-Anwendungen unnötig lange warten. Mögliche Einstellungen sind `YES` oder `NO`.

```
UseProxy YES
```

### ProxyScanners

Anzahl der AV-Scanner im Pool (siehe auch `UseProxy`).

```
ProxyScanners 8
```

### ProxyConnections

Anzahl der maximal zulässigen, gleichzeitigen Verbindungen zwischen AntiVir Milter und Scanner-Pool.

```
ProxyConnections 32
```

## 5 Konfiguration automatischer Updates

Bei einem automatischen Update werden die Bestandteile von AntiVir Milter, die den Schutz vor Viren und unerwünschten Programmen sicherstellen (vdf-Datei und Scan Engine), auf den neuesten Stand gebracht.

### 5.1 Einstellungen in antivir.conf

Die Datei /etc/antivir.conf enthält einstellbare Parameter zum automatischen Update der Scan-Engine und der Virendefinitionsdatei.

Zeilen mit # am Anfang sind Kommentare oder auskommentierte Befehle.

#### Benachrichtigungen per Email

Wenn Sie per Email über Updates benachrichtigt werden wollen, müssen Sie Ihre Email-Adresse angeben. Für diese Einstellung ist kein Standardwert vorgesehen.

Beispiel:

```
EmailTo                root@localhost
```

#### Log-Datei

Informationen über Updates können auch in einer besonderen Log-Datei gespeichert werden (ergänzend zur Ausgabe über syslog). Für diese Einstellung ist kein Standardwert vorgesehen. Beispiel:

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

#### Konfiguration des Proxy-Servers

Wenn Ihr System einen HTTP Proxy-Server verwendet, müssen Sie die Proxy-Konfiguration angeben, um Updates über das Internet zu ermöglichen. Für diese Einstellungen ist kein Standardwert vorgesehen. Beispiel:

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

## Syslog-Einstellungen

Unabhängig von den oben genannten Einstellungen gibt AntiVir wichtige Informationen über den syslog-Dämon aus. Sie können die Facility und Priorität definieren, die AntiVir diesen Informationen mitgeben soll. Wenn nicht anders definiert, gelten die folgenden Standard-Einstellungen:

SyslogFacility	user
SyslogPriority	notice

## GnuPG

AntiVir verwendet GnuPG (<http://www.gnupg.org>), um die Echtheit von Dateien bei einem Update über das Internet sicherzustellen. Damit der AntiVir Updater GnuPG nutzen kann, muss der Speicherort der Programmdateien angegeben sein (siehe Abschnitt 5.2). Wenn Sie GnuPG verwenden, muss der AntiVir Public-Key (/antivir.gpg) Ihrem PGP-Schlüsselbund hinzugefügt und unterzeichnet sein, damit die Updates durchgeführt werden können:

GnuPGBinary

Wenn Sie GnuPG verwenden, müssen Sie ggf. zusätzlich spezielle Einstellungen in Ihrem Setup angeben. Normalerweise sind solche zusätzlichen Einstellungen nicht erforderlich:

GnuPGOptions

## 5.2 AntiVir PGP Public-Key – antivir.gpg

AntiVir verwendet GnuPG (<http://www.gnupg.org>), um die Echtheit von Dateien bei einem Update über das Internet sicherzustellen. Dieses Verfahren empfehlen wir sehr. Um es zu nutzen, müssen Sie einmalig folgende Schritte durchführen:

⇒ GnuPG von der Website (<http://www.gnupg.org>) herunterladen.

Wenn Sie GnuPG und PGP zum ersten Mal verwenden, empfehlen wir Ihnen, das GnuPG-Handbuch zu lesen und sich mit dem Konzept von PGP vertraut zu machen, um eine sichere Handhabung zu gewährleisten.

⇒ Ihren eigenen PGP-Schlüssel erzeugen, wie im GnuPG-Handbuch beschrieben.

⇒ Den AntiVir PGP Public-Key Ihrem PGP-Schlüsselbund hinzufügen:

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

⇒ Fingerabdruck des Schlüssels anfordern und sicherstellen, dass dies der richtige, öffentliche AntiVir-PGP-Schlüssel ist:

```
gpg --fingerprint support@antivir.de
```

Der 40-stellige Fingerabdruck wird ausgegeben. Der öffentliche AntiVir-PGP-Fingerabdruck wird auf der AntiVir-Webseite (<http://www.antivir.de>) dargestellt. (Sie können den Fingerabdruck auch mit jemandem verifizieren, der bereits GnuPG mit AntiVir verwendet.)

- ⇒ AntiVir PGP Public-Key unterzeichnen, um seine Gültigkeit zu beglaubigen:

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

- ⇒ Sicherstellen, dass alles korrekt durchgeführt wurde, indem Sie den Fingerabdruck in der ausführbaren antivir-Datei prüfen:

- ⇒ In das Verzeichnis bin des AntiVir-Installationsverzeichnis wechseln.

Hier befinden sich zwei Dateien:

- antivir
- antivir.asc

- ⇒ Unterschrift prüfen:

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

Wenn Sie keine Fehlermeldungen erhalten, kann GnuPG für Updates über das Internet mit AntiVir Updater verwendet werden.

- ⇒ GnuPG in AntiVir aktivieren. Dazu in der Datei /etc/antivir.conf den vollständigen Pfad zur GnuPGBinary eintragen. Beispiel:

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

- ⇒ AntiVir Updater neu starten, um die geänderten Einstellungen wirksam werden zu lassen.

```
/usr/lib/antivir/avupdater restart
```

### Hinweis:

Zur Zeit wird GnuPG für Updates der AntiVir-Engine und von Programmdateien, nicht aber für die Updates von VDF-Dateien verwendet.

## 6 Vorlagen für Meldungen

Wenn Sie eine kommerzielle oder eine private Lizenz verwenden, haben Sie die Möglichkeit, eigene Meldungstexte für die Emails festzulegen, die beim Fund von Viren und unerwünschten Programmen oder bei anderen Ereignissen versandt werden.

⇒ Verzeichnis `/usr/lib/AntiVir/templates/` anlegen.

⇒ Beispiel-Vorlagen aus dem Vorlagen-Verzeichnis in das Verzeichnis `/usr/lib/AntiVir/templates/` kopieren.

⇒ Zugangsrechte festlegen:

```
chown -R uucp:uucp /usr/lib/AntiVir/templates
```

⇒ In das Verzeichnis `/usr/lib/AntiVir/templates/` wechseln. Dieses Verzeichnis enthält folgende Dateien:

- patho-administrator
- patho-recipient
- patho-sender
- virus-administrator
- virus-recipient
- virus-sender

⇒ Alle Dateien editieren und Ihren eigenen Meldungstext einfügen. Dabei den Aufbau der Dateien beachten.

- In der ersten Zeile steht der Betreff der Email.
- Anschließend folgt eine Leerzeile (neue Zeile).
- Anschließend folgt der Text der Email.

## Schlüsselwörter

Die virus-\* und patho-\*-Dateien können folgende Schlüsselwörter enthalten, die durch den entsprechenden Text ersetzt werden:

Schlüsselwort	Ersetzungstext
LICENSE	Zentrierter Lizenztext (ein bis zwei Zeilen)
SENDER	Email-Adresse des Absenders der infizierten Email
VIRUSES	Liste der Viren bzw. unerwünschten Programme, die in der infizierten Email gefunden wurden. Jede Zeile enthält den Namen eines Virus oder unerwünschten Programms, wobei Präfix und Postfix in jeder Zeile wiederholt werden
REASON	Angabe des Grundes, aus dem die Email nicht gescannt werden konnte (ein kurzer Satz)
ADVICE	Vorschlag, wie der Absender das Problem lösen kann (siehe REASON) (ungefähr eine Zeile)
QUEUEID	ID der Email in der AvMilterGate-Warteschlange
SUBJECT	Betreffzeile der infizierten Email

## Beispiel

Beispiel für eine Datei virus-recipient:

SUBJECT: AntiVir ALARM [Ihre Email: "SUBJECT"]

\*\*\*\*\*AntiVir ALARM\*\*\*\*\*

LICENSE

AntiVir hat Folgendes in der Email, die von Ihrer Adresse aus versandt wurde, entdeckt:

VIRUSES

Die Email wurde nicht zugestellt!

Diese Email wurde nicht ausgeliefert, sondern auf Ihrem Server isoliert. Überprüfen Sie bitte Ihr System unverzüglich auf eventuellen Befall mit Viren oder unerwünschten Programmen.

Bitte entfernen Sie vorhandene Viren oder unerwünschte Programme, bevor Sie weitere Emails mit Dateianhängen versenden.



**Programm & Dokumentation**  
**Copyright © 2004**  
**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 März 2004**