

Avira AntiVir Professional für UNIX

Kurzanleitung

Inhaltsverzeichnis

1. Einsatzmöglichkeiten	3
2. Installation.....	3
2.1 Manuelle Installation	3
2.2 Unbeaufsichtigte Installation.....	4
3. Empfohlene Basiskonfiguration.....	5
4. Zusätzliche Konfigurationsmöglichkeiten.....	8
4.1. Kein Echtzeitschutz	8
4.2. Hohe Auslastung des Systems.....	8
4.3. Ausnahme von Verzeichnissen	9
5. Besonderheiten – NSS Volumes.....	9
6. Kommandozeilenscanner - avscan	9
7. Updatekonfiguration	10
7.1. Sinnvolle Werte für ein Update	10
7.2. Große Unternehmen.....	10
7.3. Small Business	10
7.4. Kunden mit Schmalband Anschlüssen (Modem/ISDN).....	10
7.5. Internet Service Providers (ISPs).....	11
7.6. Signaturenupdate.....	11

1. Einsatzmöglichkeiten

- Lokaler Virenschutz

Hierbei sind lediglich die entsprechenden Shares mit DazukoFS zu mounten (bzw. als IncludePfad bei Dazuko2 zu konfigurieren).

Hinweis

Die Avira Professional Security kann sowohl mit (OnAccess) als auch ohne Echtzeitschutz (OnDemand) betrieben werden

2. Installation

2.1 Manuelle Installation

- Dekomprimieren
`gzip -d antivir-workstation-prof-3.0.2-5.tar.gz`
- Entpacken
`tar -xvf antivir-workstation-prof-3.0.2-5.tar`
- Verzeichnis wechseln
`cd antivir-workstation-prof-3.0.2-5`
- Installation ausführen
`./install\`
- Installationsdialog folgen

Folgende Abfragen sind empfohlen und sollten übernommen werden

- Would you like to setup Engine and Signature updates as cron task ? [y]
- Please specify the interval to check. Recommended values are daily or 2 hours.
available options: d [2]
- Please specify if boot scripts should be set up.
Set up boot scripts [y]

Hinweis

Für die Installation des Echtzeitschutzes unter Unix wird das externe Kernelmodul Dazuko 3.0 benötigt.

Weitere Informationen finden Sie auf der Homepage von [Dazuko](#)

2.2 Unbeaufsichtigte Installation

Wenn Sie eine komplett automatische (unattended) Installation durchführen wollen, können Sie die Installationsvariante verwenden, die auch die AMC intern verwendet.

Hierzu müssen Sie lediglich die im Installationspaket mitgelieferte SETUP.INF mithilfe des Installers wie folgt aufrufen:

```
$ ./install --fast --inf=./smcpkg/setup.inf
```

Alle Einstellungen für die automatische Installation befinden sich in der angegebenen INF Datei. Sie könnten also auch eine Kopie mit Ihren eigenen Einstellungen verwenden und so zum Beispiel einen größeren Rollout durchführen oder sich einfach die tägliche Arbeit vereinfachen.

```
./smcpkg/setup.inf:  
GUARD_INSTALL=y  
GUARD_ADDLINK=y  
GUARD_AUTOSTART=y  
GUARD_STARTNOW=y  
UPDATER_INSTALL=y  
UPDATER_ADDLINK=y  
UPDATER_AUTOSTART=ignore  
GUI_INSTALL=y  
DAZUKO_INSTALLTYPE=k  
USE_DAZUKO_LIB=2  
SAVAPI3_ADDLINK=y  
UPDATER_INSTALL=y  
UPDATER_ADDLINK=y  
UPDATER_ADDCRONJOB=y  
UPDATER_CYCLE_SIG_EN=2h  
UPDATER_CYCLE_PROD=y  
UPDATER_CYCLE=2  
UPDATER_EMAILTO=n  
SMC_INSTALL=y  
ANTIVIR_CONFIG=n  
LICENSE_AGREEMENT=y  
WRITE_FSTAB=w  
INST_DAZUKO=y
```

```
REPLACE_CRONJOB=n
REPLACE_CRONJOB_PRODUCT=n
GNOME_INSTALL=n
CONTINUE_IF_DAZUKO_FAILED=n
USE_DAZUKO2_IF_AVAILABLE=y
INST_DAZUKO=y
CREATE_QUAR_SMC=y
BIT_SUPPORT=n
FIREFOX_INSTALL=y
```

3. Empfohlene Basiskonfiguration

- **Anzahl der Scannerdaemons**

```
NumDaemons 3
```

Dies bewirkt das Starten von 3 Daemons welche für einen normalen Betrieb ausreichend sind. Die Anzahl kann bei hoher Last erhöht werden. Beachten Sie jedoch, dass hierbei genug freier Arbeitsspeicher vorhanden sein sollte!

- **Aktion bei Fund**

```
AlertAction quarantine
```

Bei einem Fund wird die Datei in das Quarantäneverzeichnis verschoben und umbenannt. Dadurch ist die Datei zum einen für den User nicht mehr zugänglich, wird aber nicht gelöscht oder verändert für den Fall, dass es sich um ein False Positive handelt.

- **Default: QuarantineDirectory NONE**

```
QuarantineDirectory/home/quarantine
```

Wenn eine Datei im /home-Verzeichnis in die Quarantäne verschoben werden soll, ist es aus Performancegründen sinnvoll, dies hier zu setzen. Statt eine große Datei von einer Partition zur anderen zu kopieren, muss diese auf der gleichen Partition einfach nur verschoben werden.

- **Zu überprüfende Dateien**

```
ScanMode all
```

Dies überprüft aus Sicherheitsgründen alle Dateien.

- **Archivüberprüfung**

```
ArchiveScan yes
```

Aktiviert das Scannen von kleineren bis mittleren Archiven. Große Archive sollten aus Performancegründen beschränkt werden – s.u.
Große Archive können z.B. mit Hilfe eines regelmäßigen Scans überprüft werden.

- **Scan in mbox**

```
MailboxScan yes
```

Führt zu einem Scan der Mailboxen. Dies sollte aus Sicherheitsgründen aktiviert sein, sofern gewünscht.

- **Maximal zu überprüfende Archivgröße**

```
ArchiveMaxSize 1GB
```

Archivbeschränkung auf insgesamt 1GB aus Performancegründen.

- **Maximal zu überprüfende Archivtiefe**

```
ArchiveMaxRecursion 20
```

Archivbeschränkung auf insgesamt 20 Ebenen aus Performancegründen.

- **Maximal zu überprüfende Kompressionsrate**

```
ArchiveMaxRatio 150
```

Archivbeschränkung auf eine Kompressionsrate von insgesamt 150 aus Performancegründen.

- **Maximal zu überprüfende Anzahl von Dateien**

```
ArchiveMaxCount 0
```

Archivbeschränkung auf eine bestimmte Anzahl von Dateien aus Performancegründen. Dies ist in der Regel nicht notwendig.

- **Benachrichtigungslevel**

```
SuppressNotificationBelow scanner warning
```

Sendet Email-Benachrichtigungen für die Komponente „scanner“ ab einem Event „warning“ und höher. Dies wird für eine ausreichende Benachrichtigung empfohlen.

- **Logdatei festlegen**

```
LogFile /var/log/avguard.log
```

Legt die Logdatei des OnAccess-Scanners fest. Dies ist der Standardpfad.

- **Erkennung von anderer bzw. ungewollter Software**

```
DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no  
hiddenext=yes joke=no pck=no phish=yes spr=no
```

Bietet per Default einen wirksamen Schutz vor ungewollter Software, wie z.B. versteckte Dateiendungen, Phishing, Dial-Up Programme, Backdoor Programme und ungewollten Werbepop-ups durch nicht gewollte Programme.

Sie können die Erkennung jedoch auch mit Hilfe der folgend aufgeführten Liste an Ihre Wünsche anpassen:

ADSPY

Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.

APPL

Eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.

BDC

Die Steuersoftware von Backdoors. BDCs sind normalerweise harmlos.

DIAL

Ein Dial-Up-Programm für kostenpflichtige Verbindungen, die riesige Rechnungen verursachen können.

GAME

Computerspiele, die eigentlich dem Computer nicht schaden.

HEUR-DBLEXT

Ausführbare Dateien, die ihre wahre Dateieindung in verdächtiger Weise verschleiern.

JOKE

Dateien mit Witzprogrammen.

PCK

Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden.

PHISH

Gefälschte E-Mails, die den Benutzer nach persönliche Informationen fragen, wie z.B. Benutzerkonto, Passwort, Online-Banking-Daten u.s.w.

SPR

Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann.

`HeuristicsLevel 2`

Aktiviert Heuristik auf Stufe Mittel:

Ein guter Mix zwischen Erkennung und Früherkennung. Dies verhindert eine Vielzahl möglicher False Positives.

`HeuristicsMacro yes`

Aktiviert Erkennung von möglichen Macrovirten in Office-Dokumenten:

Wir empfehlen den Scan in Office-Dokumenten für eine bestmögliche Überwachung.

4. Zusätzliche Konfigurationsmöglichkeiten

4.1. Kein Echtzeitschutz

Für einen reinen Kommandozeilenscanner ohne Echtzeitschutz kann der Parameter „OndemandMgmt yes“ in der `/etc/avguard.conf` gesetzt werden. Dies führt dazu, dass Dazuko bzw. DazukoFS nicht extra geladen werden muss.

4.2. Hohe Auslastung des Systems

Je nach Auslastung kann zur Performancesteigerung beim Parameter `NumDaemons` ein Wert zwischen 3 und 20 gewählt werden. Die dabei gewählten Einstellungen sollten im Verhältnis des Bedarfs und dem verfügbaren Arbeitsspeicher abgewogen werden.

4.3. Ausnahme von Verzeichnissen

Generell sollten Ausnahmen auf Datenbankverzeichnisse gesetzt werden, da diese aufgrund der internen Struktur nicht korrekt gescannt werden und außerdem massive Performanceprobleme verursachen können.

Die Ausnahmen können mit dem Parameter `ExcludePath` gesetzt werden.

Beispiel:

```
/etc/avira/avguard.conf
```

```
ExcludePath /dbdir
```

5. Besonderheiten – NSS Volumes

Der NSS startet z.B. unter SLES sehr spät. Dies führt dazu, dass das bereits gemountete DazukoFS vom NSS überlagert wird und damit nicht mehr korrekt arbeitet.

Daher ist es notwendig die Runlevel so anzupassen, dass die betroffenen Shares nach dem Start des NSS mit DazukoFS gemountet werden. Nähere Informationen zur Anpassung der Startreihenfolge entnehmen Sie bitte der jeweiligen Betriebssystemdokumentation.

6. Kommandozeilenscanner - avscan

Das `avscan`-Binary bietet den OnDemand-Scanmodus und kann unter `/usr/lib/AntiVir/avscan` mit beliebigen Parametern aufgerufen werden.

Der folgende Aufruf ähnelt der oben beschriebenen Guard-Konfiguration. Die Parameter lassen sich entsprechend ableiten. Der Scan selbst wird im `/home` Verzeichnis ausgeführt.

Der Parameter `-s` steht für eine rekursive Suche in Unterverzeichnissen. Um den Scan automatisch ohne Userinteraktion durchzuführen, kann der Parameter `--batch` verwendet werden. Funde werden so automatisch in die Quarantäne verschoben:

```
$ avscan --scan-in-archive=yes --scan-in-mbox=yes --archive-max-size=0 --archive-max-recursion=0 --archive-max-ratio=0 --scan-mode=all --heur-macro=yes --heur-level=2 --alert-action=quarantine --quarantine-dir=/home/quarantine -s --batch /home
```

Dies kann auch mittels Cronjob automatisiert werden. Es ist empfehlenswert den Aufruf in Form eines Shell-Skriptes zu erstellen und entsprechend per Cronjob aufzurufen – z.B. 1x wöchentlich am Samstag um 12 Uhr:

```
00 12 * * 6 root /usr/local/bin/virenskan.sh
```

7. Updatekonfiguration

Um Ihre AntiVir Installation auf den aktuellen Stand zu halten, werden zwei Arten von Updates bei der Installation eingerichtet:

- Scannerupdate (nur Scanner & Engine & VDF)
- Produktupdate (Guard Programmdateien)

Die Einstellungen für das Update finden Sie nach der Installation in folgender Datei:

/etc/cron.d/avira_updater

```
00 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
15 12 * * Tue root /usr/lib/AntiVir/avupdate --product=Guard
```

7.1. Sinnvolle Werte für ein Update

Je nach Zielgruppe empfehlen wir unseren Kunden mindestens 2-3 mal am Tag, ein Update durchzuführen.

7.2. Große Unternehmen

Beispiel: jede Stunde

/etc/cron.d/avira_updater

```
* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.3. Small Business

Beispiel: alle 3 Stunden

/etc/cron.d/avira_updater

```
* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.4. Kunden mit Schmalband Anschlüssen (Modem/ISDN)

Beispiel: alle 8 Stunden

/etc/cron.d/avira_updater

```
* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.5. Internet Service Providers (ISPs)

Für Internet Service Provider empfiehlt es sich natürlich, deutlich öfter nach neuen Signaturen zu schauen. Daher sollte die Frequentierung der Updateaufrufe deutlich höher angelegt sein, z.B. alle 15 Minuten. So ist sichergestellt, dass Sie immer zeitnah die neuesten Signaturen einsetzen.

```
/etc/cron.d/avira_updater
```

```
* /15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner
```

7.6. Signatureupdate

Es gibt darüber hinaus die Möglichkeit, ein reines Engine- und VDF- Update durchzuführen. Die Guard Produkdateien, sowie der zentrale Scannerdienst (SAVAPI) werden dabei nicht mitaktualisiert.

Dies kann im Allgemeinen sehr interessant für Sie sein, wenn Sie Programmupdates als besonders sensitiv betrachten. Dadurch erhalten Sie die Möglichkeit, auf einem separaten Testsystem zunächst einen Audit durchzuführen, bevor Sie die neue Version produktiv einsetzen.

Der Aufruf dafür lautet:

```
$ /usr/lib/AntiVir/avupdate --product=Signatures
```

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

Ausgabe Q4-2011

Hier verwendete Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.



live free.™