

SOPHOS

Sophos Endpoint Security and Control 9.5 Startup-Anleitung für Linux, NetWare und UNIX

Stand: Juni 2010



Inhalt

1	Einleitung.....	3
2	Systemvoraussetzungen.....	4
3	Schützen von Linux-Systemen.....	5
4	Schützen von NetWare-Servern.....	7
5	Schutz von UNIX-Systemen.....	9
6	Schützen von UNIX-Systemen mit Sophos Anti-Virus 4.....	10
7	Schützen von UNIX-Systemen mit Sophos Anti-Virus 7.....	12
8	Überprüfen der Netzwerkintegrität.....	16
9	Technischer Support.....	17
10	Rechtlicher Hinweis.....	18

1 Einleitung

In dieser Anleitung wird die Installation von Sophos Anti-Virus auf Linux-, NetWare- und UNIX-Computern für die Verwaltung durch Sophos Enterprise Console erläutert. In dieser Anleitung wird davon ausgegangen, dass Sie die Management-Tools installiert haben. Anweisungen hierzu entnehmen Sie bitte der *Sophos Endpoint Security and Control Erweiterte Startup-Anleitung*.

Upgrades werden in der *Sophos Endpoint Security and Control Upgrade-Kurzanleitung* und in der *Sophos Endpoint Security and Control Erweiterte Upgrade-Anleitung* beschrieben.

Sophos Begleitmaterial ist auf <http://www.sophos.de/support/docs/> und auf den Sophos CDs erhältlich.

2 Systemvoraussetzungen

Die Systemanforderungen entnehmen Sie bitte der Sophos Website:

<http://www.sophos.de/products/all-sysreqs.html>.

Zum Herunterladen der Software von der Sophos Website ist eine Internetverbindung erforderlich.

3 Schützen von Linux-Systemen

Zum Schutz von Linux-Systemen sind folgende Schritte erforderlich:

- Erstellen eines Installationspakets
- Installation von Sophos Anti-Virus auf Linux-Systemen

3.1 Erstellen eines Installationspakets

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus anhand der Anweisungen in der *Erweiterten Startup-Anleitung* zu *Sophos Endpoint Security and Control* heruntergeladen haben.

Mithilfe des Skripts **mkinstpkg** können Sie ein Distributionspaket für Ihre Benutzer erstellen. Das Skript benötigt Informationen darüber, wie Sophos Anti-Virus auf Ihren Linux-Computern installiert wird. Die Antworten werden in das Installationspaket eingefügt. Wenn die Benutzer eine Installation über dieses Paket vornehmen, müssen Sie keinerlei Informationen bereitstellen, da Update-Speicherort und Zugangsdaten automatisch korrekt eingerichtet werden. Sie können ein Paket in Form eines tar-Archivs oder im RPM-Format erstellen.

Hinweis: Das Skript **mkinstpkg** ist nur für den unternehmensinternen Gebrauch bestimmt. Lesen Sie bitte den vom Skript **mkinstpkg** angezeigten Lizenzvertrag und den rechtlichen Hinweis.

So erstellen Sie ein Installationspaket:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.

- b) Notieren Sie sich die entsprechenden Pfade.
2. Melden Sie sich am Linux-Server als „root“ an.
3. Mounten Sie das Bootstrap-Verzeichnis.
(Damit dieses Verzeichnis automatisch beim Systemstart gemountet werden kann, verwenden Sie dazu distributionsspezifische Tools oder bearbeiten Sie „fstab“.)
4. Ändern Sie das Bootstrap-Verzeichnis.
5. Um ein Installationspaket in Form eines tar-Archivs namens savinstpkg.tgz zu erstellen, geben Sie Folgendes ein:

```
./mkinstpkg.sh
```

Um ein Installationspaket im RPM-Format namens savinstpkg-0.0-1.i586.rpm zu erstellen, geben Sie Folgendes ein:

```
./mkinstpkg.sh -r
```

Hinweis: Der Dateiname wird vom RPM-Setup bestimmt und kann daher etwas anders aussehen.

6. Wählen Sie die Verwaltung von Computern über Enterprise Console.
7. Als Speicherort geben Sie das Bootstrap-Verzeichnis an (wie es von den Linux-Computern gesehen wird).

Jetzt können Sie Sophos Anti-Virus über das Installationspaket installieren.

3.2 Installieren von Sophos Anti-Virus über das Installationspaket

Über das Installationspaket können Sie Sophos Anti-Virus anhand einer der folgenden Methoden installieren:

- Manuelle Installation auf allen Computern. Diese Methode ist über ein RPM-Paket oder ein tar-Archiv möglich.
- Automatische Installation im gesamten Netzwerk. Diese Methode ist nur über ein RPM-Paket möglich.

3.2.1 Manuelles Installieren von Sophos Anti-Virus

1. Verwenden Sie Ihre eigenen Tools, um das Installationspaket auf die Computer zu kopieren, auf denen Sie Sophos Anti-Virus installieren möchten.
2. Gehen Sie zu jedem Computer und melden Sie sich als Root an.
3. Legen Sie das Installationspaket in einem temporären Verzeichnis ab und wechseln Sie zu diesem Verzeichnis.
4. Um eine Installation über das tar-Paket durchzuführen, geben Sie Folgendes ein:

```
tar -zxvf savinstpkg.tgz
./sophos-av/install.sh
```

Um eine Installation über das RPM-Paket durchzuführen, geben Sie Folgendes ein:

```
rpm -i RPM-Paket
```

Die erforderlichen Dateien werden vom Server kopiert und Sophos Anti-Virus wird installiert. Sophos Anti-Virus wird von nun an bei jedem Update des Bootstrap-Verzeichnisses automatisch upgedatet.

3.2.2 Automatisches Installieren von Sophos Anti-Virus

- ❖ Wenn Sophos Anti-Virus automatisch über das Installationspaket installiert werden soll, verwenden Sie ein Betriebssystem-Verwaltungstool, das die Remote-Installation unterstützt. Weitere Informationen entnehmen Sie bitte der entsprechenden Anleitung.

Nach der Installation wird Sophos Anti-Virus gestartet und automatisch bei jedem Update des Bootstrap-Verzeichnisses upgedatet.

4 Schützen von NetWare-Servern

Führen Sie auf jedem NetWare-Server folgende Schritte aus:

- Installieren von Sophos Anti-Virus
- Laden von Sophos Anti-Virus.

4.1 Installieren von Sophos Anti-Virus

In diesem Abschnitt wird davon ausgegangen, dass Sie auf jedem NetWare-Server ein zu schützendes Verzeichnis angelegt und Sophos Anti-Virus darin abgespeichert haben, wie in der *Erweiterten Startup-Anleitung zu Sophos Endpoint Security and Control* erläutert wird.

Zur Installation von Sophos Anti-Virus führen Sie auf jedem NetWare-Server folgende Schritte durch:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.
Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.
 - b) Notieren Sie sich die entsprechenden Pfade.
2. Melden Sie sich auf einem Windows-Computer mit NetWare-Administratorsoftware mit Administratorenrechten auf dem NetWare-Server an.
3. Wechseln Sie in das Bootstrap-Verzeichnis.
4. Kopieren Sie alle Dateien aus diesem Verzeichnis nach `\\NetWare-Server\SYS\SWEET`

4.2 Laden von Sophos Anti-Virus

Führen Sie zum Laden von Sophos Anti-Virus die folgenden Schritte für alle NetWare-Server durch:

1. Führen Sie auf einem Windows-Computer, auf dem die NetWare-Administratorsoftware ausgeführt wird, folgende Schritte aus:
 - a) Fügen Sie das Standard-Installationsverzeichnis zum Suchpfad hinzu:
`SEARCH`
Die Anzahl der Zeichenketten im Suchpfad wird angezeigt. Geben Sie folgenden Befehl ein:
`SEARCH ADD nächste Zeichenkettensnummer SYS:\SWEET\`
Dabei ist die *nächste Zeichenkettensnummer* die Anzahl der Zeichenketten + 1.
 - b) Laden Sie Sophos Anti-Virus:
`LOAD SWEET`

Es empfiehlt sich, die genannten Befehle in der gleichen Reihenfolge in die Datei AUTOEXEC.NCF aufzunehmen. Auf diese Weise wird Sophos Anti-Virus bei jedem Server-Neustart neu gestartet.

Wenn Sie Sophos Anti-Virus zum ersten Mal laden, werden Sie zur Eingabe von Administratordaten aufgefordert.

2. Drücken Sie eine Taste.
3. Geben Sie den vollständigen Namen (fully qualified distinguished name) eines Administrators ein und drücken Sie die Eingabetaste.
4. Geben Sie das Administrator-Kennwort ein und drücken Sie die Eingabetaste.
Notieren Sie sich den vollständigen Namen des Administrators und das Kennwort (an einem sicheren Ort). Sophos Anti-Virus meldet sich nun bei jedem Start als Administrator an und kann so die vollständige eDirectory-Struktur sehen.

Das **Sophos Anti-Virus**-Fenster wird geöffnet.

Das Laden von Sophos Anti-Virus ist abgeschlossen. Sophos Anti-Virus wird ab jetzt bei jedem Update des Bootstrap-Verzeichnisses automatisch aktualisiert.

5 Schutz von UNIX-Systemen

Für UNIX-Systeme gibt es zwei Versionen von Sophos Anti-Virus.

Sophos Anti-Virus, Version 4

Diese Version weist folgende Merkmale auf:

- Unterstützung einer Vielzahl von Plattformen (siehe <http://www.sophos.de/products/all-sysreqs.html>).
- Die Verwaltung über Enterprise Console ist nicht möglich.
- Automatische Updates sind nicht möglich.
- Geplante Scans sind nicht möglich (Ausnahme: „cronab“-Befehl).

Der Schutz von UNIX-Systemen mit Version 4 wird im Abschnitt *Schützen von UNIX-Systemen mit Sophos Anti-Virus 4* (Seite 10) beschrieben.

Sophos Anti-Virus, Version 7

Diese Version weist folgende Merkmale auf:

- Unterstützung einer kleinen Anzahl von Plattformen (siehe <http://www.sophos.de/products/all-sysreqs.html>).
- Die Verwaltung über Enterprise Console ist möglich.
- Automatische Updates sind möglich.
- Geplante Scans sind möglich.

Der Schutz von UNIX-Systemen mit Version 7 wird im Abschnitt *Schützen von UNIX-Systemen mit Sophos Anti-Virus 7* (Seite 12) beschrieben.

6 Schützen von UNIX-Systemen mit Sophos Anti-Virus 4

Folgende Schritte sind erforderlich:

- Bereitstellen von Sophos Anti-Virus für UNIX auf einem Webserver.
- Installieren von Sophos Anti-Virus auf UNIX-Systemen.

6.1 Freigeben von Sophos Anti-Virus in einem Webserver

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus anhand der Anweisungen in der *Erweiterten Startup-Anleitung* zu *Sophos Endpoint Security and Control* heruntergeladen haben.

Sie müssen Sophos Anti-Virus in einem Webserver freigeben, damit Computer über HTTP darauf zugreifen können. Wenn dies bereits erfolgt ist, können Sie diesen Abschnitt überspringen.

So geben Sie Sophos Anti-Virus in einem Webserver frei:

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.
Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.
 - b) Notieren Sie sich die entsprechenden Pfade.
2. Stellen Sie das Bootstrap-Verzeichnis, einschließlich der Unterordner, auf dem Webserver bereit.
3. Legen Sie Benutzernamen und Kennwörter zum Schutz vor unerlaubtem Zugriff auf den Ordner im Webserver fest.

Hinweis: Anweisungen zur Freigabe von Ordnern im Internet und zum Einrichten von Zugangsdaten entnehmen Sie bitte dem Begleitmaterial des Webserver. Wenden Sie sich bei weiteren Fragen bitte an Ihren Webserver-Betreiber.

Installieren Sie jetzt Sophos Anti-Virus.

6.2 Installieren von Sophos Anti-Virus

Zur Installation von Sophos Anti-Virus sind auf jedem UNIX-System folgende Schritte erforderlich:

1. Öffnen Sie das Stammverzeichnis (Root) des Bootstrap-Verzeichnisses des Webserver.
2. Kopieren Sie die Datei `emininstall.sh` in einen Pfad für ausführbare Dateien, z.B. `/etc`.
Im Folgenden wird dieses Verzeichnis als *Pfad* bezeichnet.

3. Geben Sie folgenden Befehl ein:

```
cd Pfad
```

4. Geben Sie folgenden Befehl ein:

```
chmod +x emininstall.sh
```

5. Erstellen Sie im Verzeichnis */etc* eine Datei namens *emininstall.conf*.

6. Öffnen Sie diese Datei in einem Editor und geben Sie folgende Zeilen ein:

```
EM install CID=Bootstrap-Verzeichnis  
EM cache dir=Cache-Pfad  
SAV install dir=Installationspfad
```

Hierbei gilt:

- *Bootstrap-Verzeichnis* ist das auf dem Webserver freigegebene Bootstrap-Verzeichnis.
- *Cache-Pfad* ist das Cache-Verzeichnis, in das beim Update-Vorgang die Installationsdateien kopiert werden.
- *Installationspfad* ist das Verzeichnis, in das Sophos Anti-Virus installiert wird.

Hinweis: Die Dateien im *Cache-Pfad* dürfen nicht gelöscht werden, da sie sonst erneut heruntergeladen werden. Aus diesem Grund sollten Sie die Dateien nicht im */tmp*-Verzeichnis ablegen, das gelegentlich vom UNIX-System gelöscht wird.

7. Starten Sie

```
emininstall.sh
```

Die Installation von Sophos Anti-Virus ist hiermit abgeschlossen.

8. Erstellen Sie einen Cron-Job, um *emininstall.sh* in regelmäßigen Abständen auszuführen. Daraufhin sucht die Datei nach Updates und installiert sie automatisch. Näheres zur Erstellung eines Cron-Jobs entnehmen Sie bitte dem Support-Artikel 12176 (<http://www.sophos.de/support/knowledgebase/article/12176.html>) auf der Sophos Website.

7 Schützen von UNIX-Systemen mit Sophos Anti-Virus 7

Die Installation ist anhand einer der folgenden Methoden möglich:

- Installationspaket.
- Tarball.

7.1 Schützen von UNIX-Systemen über ein Installationspaket

Zum Schützen von UNIX-Systemen über ein Installationspaket sind folgende Schritte erforderlich:

- Erstmalige manuelle Installation von Sophos Anti-Virus auf einem UNIX-Server.
- Erstellen eines Installationspakets.
- Installieren von Sophos Anti-Virus auf den restlichen UNIX-Systemen.

7.1.1 Manuelle Erstinstallation von Sophos Anti-Virus

In diesem Abschnitt wird davon ausgegangen, dass Sie Sophos Anti-Virus anhand der Anweisungen in der *Erweiterten Startup-Anleitung* zu *Sophos Endpoint Security and Control* heruntergeladen haben.

Wenn Sophos Anti-Virus, Version 4, auf dem UNIX-Server installiert wurde und Sie ein Upgrade auf Version 7 durchführen möchten, muss Version 4 zunächst deinstalliert werden. Entsprechende Anweisungen entnehmen Sie bitte der *Startup-Anleitung zu Sophos Anti-Virus für UNIX*, Version 4.

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.
Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.
 - b) Notieren Sie sich die entsprechenden Pfade.
2. Melden Sie sich am UNIX-Server als „root“ an.
3. Mounten Sie das Bootstrap-Verzeichnis.
4. Ändern Sie das Bootstrap-Verzeichnis.
5. Führen Sie das Installationsskript aus:

```
./install.sh
```

Aktivieren Sie Remote-Management.

Nach dem Update wird der UNIX-Server in Enterprise Console in der Gruppe **Nicht zugewiesen** aufgeführt.

6. Erstellen Sie in Enterprise Console ggf. eine neue Gruppe für den UNIX-Server.
7. Ziehen Sie den Server aus der Gruppe **Nicht zugewiesen** in diese Gruppe.
8. Standardmäßig ist der Gruppe bereits die Standard-Update-Richtlinie zugewiesen. Anweisungen zum Ändern der Richtlinie können Sie bei Bedarf der *Hilfe* zu *Enterprise Console* entnehmen.
9. Geben Sie auf dem UNIX-Server folgenden Befehl ein, um das erste Update durchzuführen:

```
/opt/sophos-av/bin/savupdate
```

Der nächste Schritt ist die Erstellung eines Installationspakets.

7.1.2 Erstellen eines Installationspakets

Mithilfe des Skripts **mkinstpkg** können Sie ein Distributionspaket für Ihre Benutzer erstellen. Das Skript benötigt Informationen darüber, wie Sophos Anti-Virus auf Ihren UNIX-Computern installiert wird. Die Antworten werden in das Installationspaket eingefügt. Wenn die Benutzer eine Installation über dieses Paket vornehmen, müssen Sie keinerlei Informationen bereitstellen, da Update-Speicherort und Zugangsdaten automatisch korrekt eingerichtet werden. Sie können ein Paket in Form eines tar-Archivs erstellen.

Hinweis: Das Skript **mkinstpkg** ist nur für den unternehmensinternen Gebrauch bestimmt. Lesen Sie bitte den vom Skript **mkinstpkg** angezeigten Lizenzvertrag und den rechtlichen Hinweis.

So erstellen Sie ein Installationspaket:

1. Wechseln Sie auf dem UNIX-Server mit Sophos Anti-Virus in das Verzeichnis `/opt/sophosav/update/cache/Primary-unpacked`.
2. Um ein Installationspaket in Form eines tar-Archivs namens `savinstpkg.tar` zu erstellen, geben Sie Folgendes ein:

```
./mkinstpkg.sh
```
3. Wählen Sie die Verwaltung von Computern über Enterprise Console.
4. Geben Sie als Speicherort den freigegebenen Ordner an (aus Sicht eines UNIX-Systems).

Jetzt können Sie Sophos Anti-Virus über das Installationspaket installieren.

7.1.3 Installieren von Sophos Anti-Virus über das Installationspaket

Über das Installationspaket können Sie Sophos Anti-Virus anhand einer der folgenden Methoden installieren:

- Manuelle Installation auf allen Computern.
- Automatische Installation im gesamten Netzwerk.

7.1.3.1 Manuelles Installieren von Sophos Anti-Virus

1. Verwenden Sie Ihre eigenen Tools, um das Installationspaket auf die Computer zu kopieren, auf denen Sie Sophos Anti-Virus installieren möchten.

2. Gehen Sie zu jedem Computer und melden Sie sich als Root an.
3. Legen Sie das Installationspaket in einem temporären Verzeichnis ab und wechseln Sie zu diesem Verzeichnis.
4. Um eine Installation über das tar-Paket durchzuführen, geben Sie Folgendes ein:

```
tar -xvf savinstpkg.tar
./sophos-av/install.sh
```

Die erforderlichen Dateien werden vom Server kopiert und Sophos Anti-Virus wird installiert. Sophos Anti-Virus wird von nun an bei jedem Update des Bootstrap-Verzeichnisses automatisch upgedatet.

7.1.3.2 Automatisches Installieren von Sophos Anti-Virus

- ❖ Wenn Sophos Anti-Virus automatisch über das Installationspaket installiert werden soll, verwenden Sie ein Betriebssystem-Verwaltungstool, das die Remote-Installation unterstützt. Weitere Informationen entnehmen Sie bitte der entsprechenden Anleitung.

Nach der Installation wird Sophos Anti-Virus gestartet und automatisch bei jedem Update des Bootstrap-Verzeichnisses upgedatet.

7.2 Schützen von UNIX-Systemen über Tarball

7.2.1 Herunterladen des Sophos Anti-Virus-Tarballs

1. Rufen Sie <http://www.sophos.de/support/updates/> auf.
2. Geben Sie Ihre MySophos-Zugangsdaten ein.
3. Rufen Sie die Webseite für Sophos Anti-Virus für UNIX-Downloads auf und laden Sie den Sophos Anti-Virus für UNIX-Tarball herunter.
4. Der Tarball muss in einem Verzeichnis gespeichert werden, auf das die zu schützenden UNIX-Computer zugreifen können.
Sie können den Installer auch auf eine CD oder DVD brennen.

7.2.2 Installieren von Sophos Anti-Virus über Tarball

Es wird davon ausgegangen, dass Sie den Tarball und Sophos Anti-Virus anhand der Anweisungen in der *Erweiterten Startup-Anleitung* zu *Sophos Endpoint Security and Control* in eine Freigabe heruntergeladen haben.

Wenn Sophos Anti-Virus, Version 4, auf dem UNIX-Computer installiert wurde und Sie ein Upgrade auf Version 7 durchführen möchten, muss Version 4 zunächst deinstalliert werden.

Entsprechende Anweisungen entnehmen Sie bitte der *Startup-Anleitung zu Sophos Anti-Virus für UNIX*, Version 4.

1. Den Pfad zur Freigabe, in die Sophos Anti-Virus heruntergeladen wurde („Bootstrap-Verzeichnis“), können Sie wie folgt ermitteln:
 - a) Klicken Sie in Enterprise Console im Menü **Ansicht** auf **Bootstrap-Verzeichnisse**.

Im Dialogfeld **Bootstrap-Verzeichnisse** werden in der Spalte **Verzeichnis** die Bootstrap-Verzeichnisse für alle Plattformen angezeigt.

- b) Notieren Sie sich die entsprechenden Pfade.

2. Melden Sie sich am UNIX-Computer als „root“ an.
3. Entpacken Sie den im Vorfeld heruntergeladenen Tarball:

```
tar -xvf tarball
```

4. Führen Sie das Installationsskript aus:

```
./sophos-av/install.sh
```

Wenn Sie zur Angabe eines Update-Verzeichnisses aufgefordert werden, geben Sie die Adresse des Bootstrap-Verzeichnisses an.

5. Leiten Sie das erste Update folgendermaßen ein:

```
/opt/sophos-av/bin/savupdate
```

Nach dem Update befindet sich der UNIX-Computer in Enterprise Console in der Gruppe **Nicht zugewiesen**.

6. Erstellen Sie in Enterprise Console ggf. eine neue Gruppe für den UNIX-Computer.
7. Ziehen Sie den Computer aus der Gruppe **Nicht zugewiesen** in diese Gruppe.
8. Standardmäßig ist der Gruppe bereits die Standard-Update-Richtlinie zugewiesen. Anweisungen zum Ändern der Richtlinie können Sie bei Bedarf der *Hilfe* zu *Enterprise Console* entnehmen.

Der UNIX-Computer ist nun geschützt. Sophos Anti-Virus wird von nun an bei jedem Update des Bootstrap-Verzeichnisses automatisch upgedatet. Wiederholen Sie die Schritte 2 bis 8 für alle UNIX-Computer, die geschützt werden sollen.

8 Überprüfen der Netzwerkintegrität

So überprüfen Sie die Netzwerkintegrität über Enterprise Console:

❖ Öffnen Sie das Dashboard.

Wenn es nicht angezeigt wird, wählen Sie aus dem Menü **Ansicht** die Option **Dashboard**.

Im Dashboard wird angezeigt, wie viele Computer

- Bedrohungen erkannt haben.
- sich nicht auf dem neuesten Stand befinden
- nicht mit Richtlinien übereinstimmen.

9 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

10 Rechtlicher Hinweis

Copyright © 2010 Sophos Group. Alle Rechte vorbehalten. Kein Teil dieser Publikation darf in jeglicher Form, weder elektronisch oder mechanisch, reproduziert, elektronisch gespeichert oder übertragen werden, noch fotokopiert oder aufgenommen werden, es sei denn, Sie haben entweder eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit den Lizenzvereinbarungen reproduziert werden darf oder Sie haben eine schriftliche Genehmigung des Copyright-Inhabers.

Sophos und Sophos Anti-Virus sind eingetragene Warenzeichen der Sophos Plc und Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²² know.

Douglas C. Schmidt²³

Quellen

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>

18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

„This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)“

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation <<http://www.imatix.com>>.