



Sophos Anti-Virus (SAV) – Dokumentation

1. Allgemeines	2
1.1 Zusammenfassung	2
1.2 Verfügbare Produkte.....	4
1.3 Lizenzbedingungen.....	5
1.4 Hinweise zur Benutzung.....	5
1.5 Hinweise zu Windows XP Home Edition	6
2. Download der Software vom Server des RRZK.....	7
2.1 Download	7
2.2 Versionen und Dateinamen	7
2.3 Zeitplan für die Versionen von SAV.....	8
3. Installation.....	8
3.1 Allgemeines.....	8
3.2 Lokale Installation	9
3.3 Installation mit der Enterprise Console (EC).....	9
4. Aktualisieren eines lokal installierten SAV	10
4.1 Allgemeines.....	10
4.2 Rechner im UKLAN - Versionen für Windows, Linux und MacOS-X.....	10
4.3 Mobile Rechner und Rechner außerhalb des UKLAN	12
5. Automatische Aktualisierung von Netzwerkinstallationen.....	14
5.1 Sophos Enterprise Console (EC).....	14
6. Dokumentation.....	15
7. Problem-Meldungen	15



1. Allgemeines

Kontakt

Bei Fragen oder Problemen wenden Sie sich bitte unter Angabe von Betriebssystem (etwa Windows XP Pro mit Service Pack 2), SAV-Version (etwa SAV 10.2), eingesetzter beziehungsweise aktivierter Firewall (etwa Sophos Client Firewall) und der Fehlermeldung beziehungsweise Angabe der Protokoll-Datei per E-Mail an sophosmgr@uni-koeln.de.

Bei lizenzrechtlichen Fragen wenden Sie sich bitte an softwaremgr@uni-koeln.de.

Laufzeit

Laufzeit des aktuellen Vertrages bis: 31.12.2016

Links zu Sophos u.a.

Sophos-Download-Verzeichnis des RRZK (nur im UKLAN lesbar):

<https://lizenzsoftware.uni-koeln.de/sophos/>

Benutzerdaten für Updateserver (nur im UKLAN lesbar):

<http://rrzk.uni-koeln.de/11538.html>

Webseite der Firma Sophos:

<http://www.sophos.de/>

Download der Virendefinitionen bei Sophos:

<http://www.sophos.de/downloads/ide/>

Download der SAV Dokumentation bei Sophos:

<http://www.sophos.com/de-de/support/documentation.aspx>

1.1 Zusammenfassung

Das für Endbenutzer zentrale Programm der Firma Sophos ist Sophos Anti-Virus (SAV) beziehungsweise Sophos Endpoint Security and Control (Windows) zur Abwehr von Computer-Viren und anderen Schädlingen. SAV kann entweder vom Benutzer "lokal" installiert werden (das heißt direkt auf seinem Rechner) oder aber zentral mit Hilfe der Enterprise Console in einem Netzwerk auf mehrere Rechner verteilt und konfiguriert werden.



Stand: Januar 2013

Lokale Installation

Für die lokale Installation muss das Installationspaket von SAV einmal von unserem Software-Server herunter geladen werden. Das lokal installierte SAV ist so konfiguriert, dass es sich automatisch in festen Zeitintervallen (60 Minuten) über einen unserer Update-Server aktualisiert und keine manuellen Eingriffe mehr notwendig sind. Zudem kann das Aktualisieren jederzeit manuell angestoßen werden. Daher ist es nicht notwendig, zur lokalen Installation die aktuellste Version von SAV zu benutzen.

Neue Versionen werden bei wichtigen Änderungen auf unserem Download-Server bereitgestellt. Wenn Sie auf eine neue Version wechseln möchten, ändern Sie bitte mit administrativen Rechten in der Sophos Update Konfiguration die Updateserver, indem Sie die Updateserver der alten Version durch die Updateserver der neuen Version ersetzen. Die Installation der neuen Version wird beim nächsten Update automatisch durchgeführt.

Neben SAV kann die Sophos Client Firewall (SCF) von Interesse sein, die ein installiertes SAV voraussetzt und unerwünschte Zugriffe aus dem Internet zum Rechner oder vom Rechner in das Internet (zum Beispiel bei Trojanern) verhindern kann. Im Allgemeinen sollte es aber reichen, die Firewall von Windows zu aktivieren.

Die einzelnen Arbeitsschritte für die lokale Installation und Konfiguration von SAV auf einem PC unter Windows:

- Notieren der Benutzerdaten für den Update-Webserver (vergleiche Abschnitt 4.).
- Herunterladen der Installationspakets, zum Beispiel „escw_100_sa_sfx.exe“.
- Starten dieser Datei mit Administratorrechten durch Doppelklick und Installieren von SAV, dabei Vorgaben akzeptieren.
- Sobald der Dialog "Eigenschaften von Sophos AutoUpdate" erscheint, die Adresse des Servers sowie Benutzername und Kennwort der Benutzerdaten eingeben.
- Mit Klick auf [OK] bestätigen. (Die restlichen (Vor-) Einstellungen werden damit übernommen.)



Stand: Januar 2013

- Erste Aktualisierung durch Doppelklick auf den blau-weißen Sophos-Schild in der Windows-Symbolleiste starten.

Automatische Verteilung in einem Netzwerk

Ein Werkzeug für Netzadministratoren und PC-Pool-Betreuer ist die Enterprise Console (vergleiche Abschnitt 5.), mit der SAV und SCF in einem lokalen Netzwerk verteilt, konfiguriert und aktualisiert werden können.

1.2 Verfügbare Produkte

Der Vertrag mit der Firma Sophos (Laufzeit s. oben) umfasst die folgenden Produkte für Betriebssysteme wie Linux, MacOS-X oder Windows:

- Sophos Anti-Virus (SAV) für Linux, MacOS-X, Unix und Windows
- Sophos Anti-Virus Interface für die Integration von SAV in andere Anwendungen
- Sophos Mobile Security
- Sophos E-Mail Appliances-Software
- Sophos PureMessage für Windows/Exchange (Anti-Virus, Anti-Spam & Extended Policy Modul)
- Sophos PureMessage für Unix (Anti-Virus, Anti-Spam & Extended Policy Modul)
- Sophos Client Firewall (Windows; die Firewall setzt die Installation von SAV voraus)
- Enterprise Console (EC), ermöglicht die automatische Verteilung, Administration und Aktualisierung von SAV und SCF in lokalen Netzwerken.

(Interessenten für PureMessage oder Mailmonitor wenden sich bitte an den oben genannten Kontakt.)

Der Vertrag erlaubt insbesondere, Sophos Anti-Virus (SAV) auf Rechnern in der Universität und auf Privatrechnern von Angehörigen der Universität zu Köln einzusetzen.

SAV wird vom RRZK sowohl in der Enterprise Console als auch auf den Update-Servern für die nachfolgend angegebenen Betriebssysteme stündlich aktualisiert (entsprechend konfigurierte Installationen werden im gleichen Rhythmus automatisch aktualisiert):



Stand: Januar 2013

- Windows 2000/XP/2003/Vista/2008/Windows 7
- MacOS-X
- Linux Intel

Zudem wird SAV für diese Plattformen zum Download im UKLAN bereit gestellt. Von außerhalb des UKLAN ist das Aktualisieren oder Herunterladen nur mit einem Benutzerkonto des RRZK möglich.

1.3 Lizenzbedingungen

Mit dem Herunterladen der Software erkennen Sie die Lizenzbedingungen der Firma Sophos sowie die allgemeinen Lizenzbedingungen des RRZK (wie auf unseren Webseiten veröffentlicht) an: Der Einsatz der Sophos Software ist nur auf Rechnern von Einrichtungen und Angehörigen (das sind Mitarbeiter und Studierende) der Universität zu Köln erlaubt. Die Weitergabe an Dritte ist verboten.

1.4 Hinweise zur Benutzung

Erkennen unter Windows, ob Sophos AV aktiv ist

Sophos AV besteht aus zwei Komponenten:

- On-Access-Scanner (prüfen beim Zugriff)
- On-Demand-Scanner (prüfen auf Befehl)

Der On-Access-Scanner prüft als Windows-Dienst jede Datei, die geöffnet wird, etwa beim Lesen einer E-Mail oder beim Bearbeiten einer Textdatei. Der On-Demand-Scanner kann z.B. über Start, Programme, Sophos Anti-Virus aufgerufen werden, um die Dateien der Festplatte oder eines Ordners gezielt zu prüfen (zu "scannen"), ohne jede einzelne Datei öffnen zu müssen.

Der On-Access-Scanner sollte immer aktiv sein. Zu erkennen ist dies am Sophos-Symbol in der Taskleiste: SAV ist aktiv, wenn das Schild-Symbol blau ist. Ist das Symbol grau, so ist der Dienst deaktiviert worden und sollte – notfalls durch einen Neustart von Windows – unbedingt aktiviert werden, um den Schutz des Rechners wieder herzustellen. Kann er nicht aktiviert werden, könnte ein Virus die Ursache sein und der Rechner sollte bis zur Klärung oder Beseitigung vom Netz genommen werden.



Stand: Januar 2013

Aktualisieren

Der mögliche Schutz ist nur gegeben, wenn SAV regelmäßig automatisch aktualisiert wird (siehe Abschnitt 4). Dies bezieht sich insbesondere auf neue Virendefinitionen. Absolute Sicherheit vor Viren ist aber nicht möglich.

Entfernen von Malware

Ist ein Rechner von einem Virus befallen, so kann in vielen Fällen SAV je nach Konfiguration (siehe Befehl "Konfigurieren, On-Access-Überprüfung" in SAV) den Virus melden, verschieben, umbenennen oder auch löschen.

Einige Viren unter Windows können nur mit speziellen Programmen im "geschützten Modus" von Windows beseitigt werden. In solchen Fällen finden Sie spezielle Programme sowie Informationen zum Säubern des Rechners bei den Herstellern von Anti-Viren-Programmen, unter anderem auch bei Sophos. In schwierigen Fällen hilft auch die Benutzerberatung RRZK. (Notieren Sie für die Suche nach den passenden Informationen oder Fragen an die Benutzerberatung den von SAV gemeldeten Namen des Virus.)

1.5 Hinweise zu Windows XP Home Edition

In der Standardinstallation ist bei Windows XP Home Edition die Benutzerverwaltung nicht aktiviert. Jeder Benutzer des Rechners arbeitet dann mit Administrator-Rechten. Dies bedeutet einerseits, dass jeder Benutzer Programme installieren kann, und andererseits, dass auch jeder Virus, der über eine E-Mail oder eine Website auf den Rechner gelangt, sich selbst installieren und gegebenenfalls den Virenschanner deaktivieren kann.

Daher sollte auch unter Windows XP Home Edition eine Benutzerverwaltung eingerichtet und nur als Benutzer mit eingeschränkten Rechten gearbeitet werden. Die Benutzerverwaltung unter XP Home Edition wird aufgerufen, wenn Windows im abgesicherten Modus gestartet wird (Funktionstaste <F8> beim Starten drücken). Für alle Benutzer (auch für den voreingerichteten Administrator) sollten unbedingt Passwörter vergeben werden. Zudem ist es sinnvoll, einen Benutzer Admin mit Administrator-Rechten einzurichten, der dann auch auf dem Begrüßungsbildschirm erscheint und im normalen Windows-Modus für Installationen etc. verwendet werden kann.



Stand: Januar 2013

Auch unter XP Home kann Sophos installiert werden. Auf einem Testrechner mit XP Home im RRZK, bei dem eine Benutzerverwaltung wie gerade beschrieben eingerichtet war, gab es weder mit dem On-Access- noch mit dem On-Demand-Scanner Probleme. Laut Rückmeldungen von Benutzern mit XP Home (ohne Benutzerverwaltung) ist nach der Installation zwar der On-Access-Scanner aktiviert, so dass der wesentliche Schutz besteht, der Aufruf des On-Demand-Scanners soll aber fehlschlagen, da "keine ausreichenden Rechte" vorhanden seien.

Falls keine anderen Ursachen vorliegen, könnte in solchen Fällen die Einrichtung der Benutzerverwaltung Abhilfe bringen.

2. Download der Software vom Server des RRZK

2.1 Download

Für lokale Installationen muss SAV einmal mit einem Browser vom Lizenzsoftware-Server des RRZK herunter geladen werden. Alternativ kann SAV in lokalen Netzwerken mit der Enterprise Console verteilt werden. Nach der Installation oder Verteilung kann SAV automatisch aktualisiert werden (Autoupdate-Funktion). Die URL des Download-Verzeichnisses finden Sie am Beginn dieser Dokumentation.

Innerhalb des UKLAN, also auch bei Benutzung von VPN, ist der Zugriff nicht eingeschränkt. Von außerhalb des UKLAN kann SAV aber nur nach Angabe von Benutzername und Passwort einer Benutzungsgenehmigung (Uni- oder SMail-Account) des RRZK herunter geladen werden.

Auf dem Server sind folgende Unterverzeichnisse angelegt:

Verzeichnis Firewall: Enthält die "Sophos Client Firewall" für Windows.

Betriebssystem spezifische Verzeichnisse Macintosh, Unix und Windows: Sie enthalten Sophos Anti-Virus (SAV) für das betreffende Betriebssystem. Im Verzeichnis Unix sind auch die Linux-Versionen, in Windows auch diejenigen für Windows Server bereitgestellt.

In Tools-emi ist die Enterprise Console (EC) zu finden, ein Programm für Windows-Server zum Verteilen und Aktualisieren von SAV in Netzwerken.

2.2 Versionen und Dateinamen



Stand: Januar 2013

SAV ist auf unserem Software-Server für unterschiedliche Betriebssysteme im zugehörigen Unterverzeichnis bereitgestellt. In den entsprechenden Verzeichnissen finden Sie die jeweils benötigte Installationsdatei.

- Esc_w_102_sa_sfx.exe: Sophos Antivirus 10.2 für Windows
- escw_100_sa_sfx.exe: Sophos Anti-Virus 10.0 für Windows
- escw_90_sa_sfx.exe: Sophos Anti-Virus 9.x für Windows
XP/2000/2003/Vista/2008/Windows 7
- savosx80sa.10.8+.dmg: SAV 8.x für MacOS-X
- sav-linux-6-i386.tgz: Linux für Intel-Plattform

Hinweis: Die aktuellen Versionen von SAV sind mit integrierter Auto-Update-Funktion versehen. Es werden daher nicht unbedingt die aktuellsten Versionen bereitgestellt, sondern ggf. die letzte stabile Version.

2.3 Zeitplan für die Versionen von SAV

Einige "alte" Versionen wie z.B. die Versionen für MacOS 8/9 oder DOS sind bereits eingestellt worden, für andere wird der Support in absehbarer Zeit enden. Genaue Angaben hierzu finden Sie unter <http://www.sophos.de/support/timeline.html>.

3. Installation

3.1 Allgemeines

Vor der Installation von SAV muss jede andere Anti-Viren-Software deinstalliert werden.

Unter Windows kann es vorkommen, dass trotz Deinstallation anderer Antivirus-Software die Installation von SAV mit der Meldung "Installation konnte nicht fortgesetzt werden, da ein anderes Anti-Viren-Programm auf diesem Computer existiert." abgebrochen wird. Suchen Sie in diesem Fall bitte mit Administratorrechten im Verzeichnis C:\Windows\Temp (im Windows-Installations-Verzeichnis\Temp) nach der Datei „Sophos AntiVirus Competitorlist.txt“. Dort wird normalerweise



Stand: Januar 2013

protokolliert, welcher Registry-Eintrag die Installation verhindert. Dieser Eintrag muss dann gelöscht werden.

Startup-Anleitungen für die Installation und Handbücher für die Konfiguration und Benutzung finden Sie auf den Webseiten der Firma Sophos.

Bei der Installation werden zwei Fälle unterschieden: die lokale (Einzelplatz-) Installation und die Installation und Verteilung mit Hilfe der Enterprise Console (Netzwerk-Installation).

In allen Fällen muss während oder auch nach der Installation die "AutoUpdate-Funktion" von SAV konfiguriert werden (vergleiche Abschnitt 4 und 5).

3.2 Lokale Installation

Die lokale Installation ist für nicht fest in ein Netzwerk integrierte oder mobile Rechner gedacht. Nach dem Download und Entpacken des Archivs wird SAV entsprechend der üblichen Installation von Software auf Ihrem Betriebssystem installiert. Hierbei kann zuerst einmal das Konfigurieren der AutoUpdate-Funktion übersprungen und später nachgeholt werden.

Nach der Installation muss SAV (im Startmenü) aufgerufen und das Verhalten beim Überprüfen von Dateien konfiguriert werden (Menü Konfigurieren, On-Access-Überprüfung oder Konfigurieren, On-Demand-Erweiterungen und -Ausnahmen), wobei u.a. die Maßnahmen (Umbenennen, Verschieben, Löschen) beim Entdecken eines Virus festgelegt werden.

Die aktuellen Versionen von SAV für Windows, MacOS-X und Linux besitzen eine AutoUpdate-Funktion, mit der SAV automatisch in festen Zeitabständen aktualisiert wird. (Unter Windows: Aufruf von Sophos Endpoint Security and Control über das Startmenü, dann Befehl "Updates konfigurieren".) Einzugeben ist dann nur die Update-Server-Adresse und ggf. ein "Update-Account" (vgl. Abschnitt 4).

Für die lokale Installation finden Sie anschauliche Kurzanleitungen für Windows und MacOS-X als PDF und Videodateien auf unseren Webseiten.

3.3 Installation mit der Enterprise Console (EC)

Das Verteilen, Installieren und Aktualisieren von SAV in einem Netzwerk kann mit der Enterprise Console (EC) sehr vereinfacht werden. Details dazu finden Sie in der Sophos Anti-Virus Startup-Anleitung esav_sde.pdf, die ebenfalls im Unterverzeichnis tools-eml des Download-Verzeichnisses zu finden ist (vgl. auch Abschnitt 5).



4. Aktualisieren eines lokal installierten SAV

4.1 Allgemeines

Das Programm Sophos Anti-Virus selbst (die Detection Engine) und vor allem die Virenkennungen (Virendefinitionen, Virensignaturen, ide-Dateien) müssen regelmäßig aktualisiert werden, um möglichst großen Schutz zu erhalten. Ein absoluter Schutz ist nicht möglich. Am sinnvollsten ist es, in festen Zeitabständen von z.B. 60 Minuten automatisch überprüfen zu lassen¹, ob neue Virenkennungen oder neue Programmversionen installiert werden können. In manchen Fällen muss nach dem Update auf eine neue Programmversion unter Windows ein Neustart des Systems durchgeführt werden.

Der Dialog zur Konfiguration der AutoUpdate-Funktion wird unter Windows durch den Aufruf von Sophos Endpoint Security and Control über das Startmenü, dann Befehl "Updates konfigurieren" geöffnet. Für andere Betriebssysteme beachten Sie bitte unsere Kurzanleitungen bzw. die ausführlichen Dokumentationen des Herstellers.

SAV muss durch Herunterladen neuer Programmversionen und neuer Virensignaturen regelmäßig aktualisiert werden. Beachten Sie dazu bitte unbedingt auch die ausführlichen Dokumentationen des Herstellers.

Wichtig bei der Konfiguration ist die Angabe der Server, von denen die Updates bezogen werden sollen. Es können bis zu zwei Server angegeben werden, ein Primary Server und ein Secondary Server. Beim Updateversuch fragt SAV zuerst den Primary Server ab und anschließend, falls kein Kontakt zustande kommt, den Secondary Server. Ausreichend ist prinzipiell die Angabe eines funktionsfähigen Primary Servers.

Die Auto-Update-Funktion aktualisiert Programm und ide-Dateien.

4.2 Rechner im UKLAN - Versionen für Windows, Linux und MacOS-X

SAV mit AutoUpdate-Funktion kann sich automatisch aktualisieren, wenn der Rechner über eine Netzwerk- oder Internet-Verbindung verfügt. Die Funktion muss bei der Installation oder später z.B. so konfiguriert werden, dass sie in einem festen Zeitintervall auf den eingerichteten Update-Servern

¹ Das Zeitintervall von 60 Minuten ist bei der Installation bereits voreingestellt und sollte nicht verändert werden.



Stand: Januar 2013

des RRZK nach Updates sucht. Anzugeben ist hierbei ein Primary Server, falls vorhanden, sollte zur Sicherheit auch ein Secondary Server angegeben werden. Verwenden Sie dazu bitte die folgenden Daten:

Windows

Verwenden Sie bitte die Version Sophos Endpoint Security and Control 10.2:

Primary Server: <http://rzk-adsec4.ad.uni-koeln.de/Bootstrap-Verzeichnisse-3/SAVSCFXP/>

Secondary Server: <http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse-3/SAVSCFXP/>

Für die Version Sophos Endpoint Security and Control 10.0

Primary Server: <http://rzk-adsec4.ad.uni-koeln.de/Bootstrap-Verzeichnisse-2/SAVSCFXP/>

Secondary Server: <http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse-2/SAVSCFXP/>

Für die Version Sophos Endpoint Security and Control 9.x für Windows:

Primary Server: <http://rzk-adsec4.ad.uni-koeln.de/Bootstrap-Verzeichnisse/SAVSCFXP/>

Secondary Server: <http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse/SAVSCFXP/>

MacOS-X

Verwenden Sie bitte Sophos Anti Virus Version 8:

Primary Server: <http://rzk-adsec4.ad.uni-koeln.de/Bootstrap-Verzeichnisse/ESCOSX/>

Secondary Server: <http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse/ESCOSX/>

Linux

Verwenden Sie bitte die Version Sophos Endpoint Security and Control 9.x:

Primary Server: <http://rzk-adsec4.ad.uni-koeln.de/Bootstrap-Verzeichnisse/savlinux/>

Secondary Server: <http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse/savlinux/>



Stand: Januar 2013

4.3 Mobile Rechner und Rechner außerhalb des UKLAN

Für das Update ein Server als "Primary Server" eingerichtet (einen "Secondary Server", gibt es nicht), über den SAV bzw. Sophos Endpoint Security and Control automatisch aktualisiert werden können.

Windows

Für Windows verwenden Sie bitte die Version Sophos Endpoint Security and Control 10.2

Primary Server: <http://sophosupdate.rrz.uni-koeln.de/SAVSCFXP10.2>

Für die Version Sophos Endpoint Security and Control 10.0

Primary Server: <http://sophosupdate.rrz.uni-koeln.de/SAVSCFXP10>

Für die Version 9.x für Windows:

Primary Server: <http://sophosupdate.rrz.uni-koeln.de/SAVSCFXP>

MacOS-X

Verwenden Sie bitte Sophos Anti Virus Version 8:

Primary Server: <http://sophosupdate.rrz.uni-koeln.de/ESCOSX/>

Linux

Verwenden Sie bitte die Version Sophos Endpoint Security and Control 9.x:

Primary Server: <http://sophosupdate.rrz.uni-koeln.de/savlinux/>

Der Zugriff auf diesen Server ist nur mit den für Angehörige der Universität bereitgestellten Sophos-Benutzerdaten möglich. Diese sind nicht mit dem eigenen S-Mail- oder Uni-Account identisch. Diese Sophos-Benutzerdaten sind im Konfigurationsdialog der AutoUpdate-Funktion in Sophos Anti-Virus als Benutzername und Kennwort für den Sophos-Updateserver einzugeben.



Die Sophos-Benutzerdaten und weitere Angaben erhalten Sie unter dem nachfolgenden Link nur im UKLAN (also auch bei Benutzung von VPN) oder nach Anmeldung mit dem eigenen S-Mail- oder Uni-Account, nachdem Sie die Einhaltung der Lizenzbedingungen per Klick auf [Akzeptieren] bestätigen:

Benutzerdaten für Updateserver: <http://rrzk.uni-koeln.de/11538.html>



5. Automatische Aktualisierung von Netzwerkinstallationen

5.1 Sophos Enterprise Console (EC)

Zunächst muss die Sophos Enterprise Console vom Lizenzsoftware-Server heruntergeladen werden. Starten Sie die Installation aus dieser Datei heraus und wählen Sie die vollständige Installation aus. Dabei werden folgende Komponenten installiert: Management-Konsole, Management Server und Datenbank-Server.

Nach der Installation wird automatisch der Software-Download-Assistent gestartet. Da dieser Assistent nur den Download vom Sophos Server unterstützt, muss der Vorgang abgebrochen werden. Zur Konfiguration der Updates, starten Sie die Sophos Enterprise Console und wählen Sie im Menü Ansicht die Option Update Manager aus. Die weiteren Schritte der Konfiguration sind beschrieben in der Dokumentation (Sophos Endpoint Security and Control 10 - Erweiterte Startup-Anleitung):

http://www.sophos.com/de-de/medialibrary/PDFs/install%20guides/sesc_100_ssgeng.pdf

Im nächsten Schritt konfigurieren Sie den Update Manager auf Ihrem Server. Im Konfigurationsfenster des Update Managers wählen Sie unter Abonnements die empfohlenen Abonnements. Diese Abonnements enthalten folgende Versionen: Windows NT, Version 4; Windows 9x, Version 4; Windows 2000 und höher, Version 9; MAC OS X 10.4+, Version 7; Linux, Version 6.

Im Konfigurationsfenster des Update Managers tragen Sie unter Quellen folgende Quellen als Pfade für das Feld UNC ein:

- \\rzk-adsec4\SophosUpdate (als primary Server)
Tragen Sie als Benutzernamen ad\Uni-NV Account und als Kennwort das entsprechende Kennwort Ihres Uni-NV Accounts ein.
- \\rzk-efms4\SophosUpdate (als secondary Server)
Tragen Sie als Benutzernamen ef\Uni-NV Account und als Kennwort das entsprechende Kennwort Ihres Uni-NV Accounts ein.

Die nachfolgenden Warnungen der Sophos Konsole können ignoriert werden.

Danach werden auf Ihrem Server das Antivirus Directory und die zugehörigen Verzeichnisse automatisch erstellt. Die Aktualisierung erfolgt ebenfalls automatisch.



Stand: Januar 2013

6. Dokumentation

Die Dokumentationen für die Sophos Produkte SAV, SESC, EC, Client Firewall etc. erhalten Sie über die Webseite der Firma Sophos unter:

<http://www.sophos.de/support/docs/>

Anleitungen und weitere Hinweise finden Sie auch in den einzelnen Unterverzeichnissen unseres Download-Verzeichnisses.

7. Problem-Meldungen

Probleme mit Sophos Produkten melden Sie bitte per E-Mail an sophosmgr@uni-koeln.de unter Angabe von:

- Betriebssystem (etwa Windows XP Pro mit Service Pack 2)
- SAV-Version (etwa 10.2)
- eingesetzter bzw. aktivierter Firewall (z.B. Windows Firewall)
- Fehlermeldung bzw. Angaben der Log-Datei