

# SOPHOS

## Sophos Control Center Startup-Anleitung

Produktversion: 4.1  
Stand: Februar 2011



# Inhalt

1	Einleitung.....	3
2	Systemvoraussetzungen.....	4
3	Installation.....	5
4	Schutz von Netzwerkcomputern.....	9
5	Prüfen, ob Computer geschützt sind.....	12
6	Einrichten von E-Mail-Benachrichtigungen.....	13
7	Scannen auf potenziell unerwünschte Anwendungen.....	15
8	Umgang mit Viren.....	17
9	Einrichten der Firewall.....	18
10	Technischer Support.....	20
11	Copyright.....	21

# 1 Einleitung

In dieser Anleitung wird erläutert, wie Sie Computer im Netzwerk (Windows und Macintosh) vor Viren (einschließlich Spyware), potenziell unerwünschten Anwendungen und anderen Sicherheits-Threats schützen.

Wenn Sie über Computer verfügen, die nie mit dem Netzwerk verbunden werden, sollten Sie auch die Einzelplatz-Startup-Anleitung zu Sophos Endpoint Security and Control zu Rate ziehen.

Wenn Sie ein Upgrade von einer früheren Version von Sophos Control Center durchführen, bietet die *Upgrade-Anleitung zu Sophos Control Center* nähere Informationen.

Details zu allen Konfigurationsoptionen von Sophos Control Center, die in der vorliegenden Anleitung nicht behandelt werden, entnehmen Sie bitte der Hilfe zu Sophos Control Center.

Sophos Begleitmaterial steht auf <http://www.sophos.de/support/docs/> zum Download bereit.

## 2 Systemvoraussetzungen

Die Systemvoraussetzungen finden Sie auf der Sophos Website:

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

Außerdem benötigen Sie Internetzugang, um die Software von der Sophos Website herunterladen zu können.

Für Sophos Control Center und Server-Komponenten gelten weitere Voraussetzungen:

- Es muss Zugriff auf und über die anderen Computer im Netzwerk bestehen.
- Es empfiehlt sich der Einsatz eines Serverbetriebssystems (z.B. Windows Server 2003 oder Windows Small Business Server 2011). Ansonsten könnte die Leistung von Sophos Control Center beeinträchtigt werden.

**Wichtig:** Wenn Sie Sophos Control Center auf Windows 2008 Small Business Server (SBS) installieren, stellen Sie sicher, dass Windows Live OneCare auf dem Computer nicht installiert ist. Sie können Windows Live OneCare über das Dienstprogramm „Software“ in der Systemsteuerung deinstallieren.

Wenn Sie mit SQL Server (und nicht mit SQL Server 2005 Express, das von Sophos für Sophos Produkte verwendet wird) arbeiten möchten, installieren Sie das Programm ggf. und erstellen Sie eine SOPHOS-Instanz. Anweisungen hierzu entnehmen Sie bitte der Dokumentation zu SQL Server. Sie können sich auch an den technischen Support von Microsoft wenden.

## 3 Installation

### 3.1 Installationsvorbereitung

Stellen Sie vor der Installation von Sophos Control Center Folgendes sicher:

- Sie haben die von Sophos übermittelten Benutzerdaten zur Hand.
- Sie sind auf dem Computer, auf dem Sophos Control Center installiert werden soll, als Administrator bzw. Domänenadministrator angemeldet.

**Hinweis:** Zum Schutz von Computern in einer Arbeitsgruppe (alle Windows Plattformen) müssen zudem die im folgenden Support-Artikel dargelegten Schritte durchgeführt werden: <http://www.sophos.de/support/knowledgebase/article/29728.html>.

### 3.2 Vorbereiten von Endpoints

Stellen Sie vor der Installation von Sicherheitssoftware auf Endpoints Folgendes sicher:

- Fremdsoftware wurde von allen Computern, auf denen Sophos Anti-Virus installiert werden soll, entfernt.
- Die erforderliche Konfiguration des Betriebssystems ist erfolgt.

#### 3.2.1 Windows Vista und höher

Für den Einsatz von Sophos Anti-Virus unter Windows Vista und höher gelten folgende Zusatzvoraussetzungen:

- Stellen Sie sicher, dass der **Remoteregistrierungsdienst** läuft und als Starttyp **Automatisch** gewählt wurde. Dieser Dienst ist unter Windows Vista standardmäßig nicht aktiv. Die Dienste finden Sie unter **Start > Systemsteuerung > Verwaltung > Dienste**. Navigieren Sie in der Dienstliste zu **Remoteregistrierungsdienst** und doppelklicken Sie auf diesen Eintrag. Rufen Sie im **Eigenschaftsfenster** des Remoteregistrierungsdiensts die Registerkarte **Allgemein** auf. Klicken Sie im Feld **Starttyp** auf den Dropdown-Pfeil und wählen Sie die Option **Automatisch** aus. Klicken Sie auf **Übernehmen**. Klicken Sie auf **Start** und anschließend auf **OK**.
- Deaktivieren Sie die **Benutzerkontensteuerung**. (Pfad: **Start > Systemsteuerung > Benutzerkonten > Benutzerkontensteuerung ein- oder ausschalten**.) Nach Fertigstellung der Installation sollten Sie sie wieder aktivieren.
- Rufen Sie **Windows Firewall mit erweiterter Sicherheit** auf. (Pfad: **Start > Systemsteuerung > Verwaltung**.) Ändern Sie **Eingehende Regeln**, um folgende Elemente zu aktivieren.

Regelname	Profil
Remotedienstverwaltung (NP eingehend)	Domäne
Remotedienstverwaltung (NP eingehend)	Privat

Regelname	Profil
Remotedienstverwaltung (RPC)	Domäne
Remotedienstverwaltung (RPC)	Privat
Remotedienstverwaltung (RPC-EPMAP)	Domäne
Remotedienstverwaltung (RPC-EPMAP)	Privat

**Hinweis:** Es empfiehlt sich, die Elemente nach der Installation wieder zu deaktivieren.

### 3.2.2 Windows XP

Die folgenden Schritte müssen auf allen Windows XP-Computern mit und ohne Service Pack durchgeführt werden:

- Entfernen Sie auf Windows XP-Systemen, auf denen Sophos Client Firewall installiert werden soll, die Firewall-Software anderer Hersteller – mit Ausnahme der Windows-Firewall.
- Deaktivieren Sie die einfache Dateifreigabe.

Nähere Anweisungen hierzu finden Sie unter  
<http://www.sophos.de/support/knowledgebase/article/12837.html>.

#### Windows XP mit Service Pack 2

Wenn Windows Firewall auf einem Computer mit Windows XP Service Pack 2 aktiviert ist und Sophos Client Firewall **nicht** installiert werden soll, verfahren Sie wie folgt:

- Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
- Fügen Sie folgende Programmausnahme hinzu:

C:\Programme\Sophos\Remote Management System\RouterNT.exe

Nähere Anweisungen hierzu finden Sie unter  
<http://www.sophos.de/support/knowledgebase/article/11075.html>.

### 3.2.3 Windows Server 2003 mit Service Pack 1

Wenn die Firewall von Windows aktiviert ist, verfahren Sie wie folgt:

- Aktivieren Sie die Datei- und Druckerfreigabe für Microsoft-Netzwerke.
- Fügen Sie folgende Programmausnahme hinzu:

C:\Programme\Sophos\Remote Management System\RouterNT.exe

Nähere Anweisungen hierzu finden Sie unter  
<http://www.sophos.de/support/knowledgebase/article/11075.html>.

### 3.2.4 Windows 2000

- Entfernen Sie auf Windows 2000-Systemen, auf denen Sophos Client Firewall installiert werden soll, die Firewall-Software anderer Hersteller – mit Ausnahme der Windows-Firewall.

### 3.2.5 Windows 98 SE

- Deinstallieren Sie alle Instanzen von Sophos Anti-Virus. Die Deinstallation sollte über das Dienstprogramm „Software“ in der Systemsteuerung erfolgen.

## 3.3 Installieren von Sophos Control Center

Installieren Sie zuerst Sophos Control Center. Mit diesem Programm können Sie die Virenschutz- und Firewall-Software herunterladen, installieren und verwalten.

1. Rufen Sie die Seite mit den Sophos Produkt-Downloads auf (<http://www.sophos.de/support/updates>) und geben Sie die Zugangsdaten ein, die Ihnen von Sophos übermittelt wurden.

Folgen Sie den Links zum Herunterladen des Installers für die Sophos Small Business Solutions und führen Sie den Installer aus.

2. Bestätigen Sie im Entpackprogramm (**Sophos Small Business Edition-Installer**) das Zielverzeichnis der Installationsdateien (das Verzeichnis muss sich auf dem gleichen Computer befinden, auf dem Sophos Control Center installiert wird) und klicken Sie anschließend auf **Installieren**.
3. Klicken Sie im Eröffnungsfenster auf **Weiter**.

Es wird ein Assistent gestartet, der Sie durch die Installation leitet. Übernehmen Sie unter Beachtung der folgenden Ausnahmen die Voreinstellungen.

4. Wählen Sie als **Setup-Typ** die Option **Vollständig** aus, um das Programm mit allen Funktionen zu installieren.

**Hinweis:** Zur Verwaltung von Sicherheitssoftware über einen anderen Computer können Sie dieses Installationsprogramm auf den gewünschten Computer kopieren, ausführen und die Option **Nur Management-Konsole** auswählen.

Klicken Sie auf **Weiter** und übernehmen Sie im Assistenten wieder die Voreinstellungen.

5. Wenn die Installation abgeschlossen ist, klicken Sie auf **Beenden**. Daraufhin werden Sie automatisch abgemeldet. Wenn Sie sich später abmelden möchten, deaktivieren Sie das Kontrollkästchen **Jetzt abmelden**, bevor Sie auf **Beenden** klicken.

In einigen Fällen reicht eine Abmeldung nicht aus und es ist ein Neustart des Systems erforderlich. In diesem Fall wird das Kontrollkästchen nicht angezeigt, sondern es öffnet sich ein Fenster mit einer Aufforderung zum Neustart des Systems, den Sie allerdings auch verschieben können.

6. Melden Sie sich bei der nächsten Anmeldung unter dem gleichen Namen an wie zuvor.  
Der Sophos Assistent zum Schutz von Netzwerken wird automatisch gestartet.

Nähere Informationen zum Schutz von Computern im Netzwerk finden Sie im Abschnitt [\*Schutz von Netzwerkcomputern\*](#) (Seite 9).

## 4 Schutz von Netzwerkcomputern

Bei der ersten Anmeldung nach der Installation wird Sophos Control Center automatisch geöffnet und der Sophos Assistent zum Schutz von Netzwerken wird gestartet. Mit dem Assistenten können Sie Computer im Netzwerk schützen.

1. Klicken Sie im Eröffnungsfenster auf **Weiter**.
2. Geben Sie auf der Seite **Sophos Download-Konto** die Zugangsdaten ein, die Sie von Sophos erhalten haben. Klicken Sie anschließend auf **Weiter**.

Sophos Control Center lädt die Software in einen Ordner auf dem gerade verwendeten Computer herunter und verteilt sie auf die anderen Computer. Der Pfad zu dem Ordner variiert je nach Betriebssystem:

- Windows 2000, XP und 2003:  
C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista und höher:  
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

Wenn Sie über einen Proxyserver auf das Internet zugreifen, aktivieren Sie das Kontrollkästchen **Verbindung zu Sophos über Proxyserver herstellen** und geben Sie die Proxyserver-Details an.

3. Wählen Sie auf der Seite **Plattform-Auswahl** die Software für die Betriebssysteme auf Ihrem Computer aus.
  - Die Voreinstellung lautet **Windows 2000 und höher**.
  - Wenn Sie unter Mac OS X arbeiten, aktivieren Sie die Option **Mac OS X**. Hierdurch werden die Computer auf die Installation der Virenschutzsoftware vorbereitet.
4. Der Download-Fortschritt wird auf der Seite **Software-Download** angezeigt. Sophos Control Center lädt die Software herunter. Klicken Sie nach Abschluss des Downloads auf **Weiter**.
5. Geben Sie auf der Seite **Windows-Benutzerkonto** die Zugangsdaten eines Benutzerkontos mit Administratorrechten für alle Netzwerkcomputer und Berechtigung zur Installation von Software ein. Es handelt sich hierbei nicht um das im Vorfeld benutzte Sophos Konto. In der Regel eignet sich das Konto, über das Sie vor Beginn der Installation angemeldet waren.
6. Auf der Seite **Computer schützen** sucht der Assistent nach Computern, auf denen die Software automatisch installiert werden kann.

Auf der Seite werden ausschließlich Computer mit Windows 2000 und höher aufgeführt, da die automatische Installation unter Windows 95/98/NT und Mac OS nicht möglich ist.

Standardmäßig ist der Computerschutz für alle Computer aktiviert. Wenn bestimmte Computer nicht geschützt werden sollen, deaktivieren Sie das entsprechende Kontrollkästchen. Wenn Sie alle Kontrollkästchen aus- bzw. abwählen möchten, aktivieren/deaktivieren Sie das Kontrollkästchen der Spaltenüberschrift **Schutz**.

- Wählen Sie auf der Seite **Funktionen auswählen** die Funktionen aus, die Sie installieren möchten:

- Virenschutz (standardmäßig aktiviert)
- Sophos Client Firewall (sofern im Lizenzumfang enthalten)

**Hinweis:** Auf allen Computern, auf denen Sophos Client Firewall installiert werden soll, ist zur Aktivierung der Firewall ein Neustart erforderlich.

- Entfernen von Fremdsoftware

Klicken Sie auf **Weiter**.

- Wenn Computer in der Liste **Computer, die manuell geschützt werden müssen** aufgeführt werden, klicken Sie auf **Drucken**. Die Computerliste wird gedruckt. Sie können die Liste auch über die Option **Speichern unter** speichern oder sich die Computer notieren. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten.

Sophos Control Center installiert die Software automatisch auf den gewählten Computern.

Virenschutz- und Firewall-Software wird auf die Computer übertragen. Ein blaues Computersymbol erscheint neben dem Computernamen und in der Spalte **Auf dem neusten Stand** wird **Ja** angezeigt.

Unter [Manueller Schutz von Netzwerkcomputern](#) (Seite 10) wird der manuelle Computerschutz näher erläutert.

## 4.1 Manueller Schutz von Netzwerkcomputern

Solche Computer können manuell geschützt werden.

- Gehen Sie zu den Computern auf der im Vorfeld ausgedruckten bzw. gespeicherten Liste. Navigieren Sie zu dem Ordner, in dem Sophos Control Center Updates für die Virenschutz- und Firewall-Software bereitstellt. Standardmäßig lauten die Ordernamen:

Betriebssystem	Ordner
<b>Windows 2000 und höher</b>	\\[Servername]\sophosUpdate\CIDs\Sxxx\EECSXP
<b>Windows 98</b>	\\[Servername]\sophosUpdate\CIDs\Sxxx\ES9X
<b>Mac OS X</b>	smb://[Servername]/sophosUpdate/CIDs/Sxxx/ESCOSX

Hierbei gilt:

Sophos Control Center [Servername] steht dabei für den Namen des Computers, auf dem Sophos Control Center installiert wurde.

[Sxxx] steht für die beim Download generierte Zahl (z.B. S000).

- Doppelklicken Sie auf „setup.exe“ (unter Windows) oder „Sophos Anti-Virus.mpkg“ (unter Mac OS X).

Wenn die Installation auf Mac OS X 10.2 oder höher erfolgt, kopieren Sie die Datei „Sophos Anti-Virus.mpkg“ auf den Mac und führen Sie die Installation dort durch.

Jetzt können Sie auch Computer schützen, die nicht permanent mit dem Netzwerk verbunden sind ([Schutz von Computern ohne permanente Netzwerkverbindung](#) (Seite 11)).

## 4.2 Schutz von Computern ohne permanente Netzwerkverbindung

Computer, die nicht immer mit dem Unternehmensnetzwerk verbunden sind (z.B. Laptops, die im Büro und unterwegs eingesetzt werden), können auch geschützt werden, wenn keine Verbindung zum Unternehmensnetzwerk besteht.

Alle Computer, auf denen die Virenschutz- und Firewallsoftware installiert wurde, sind so konfiguriert, dass sie Updates direkt von Sophos beziehen, wenn keine Verbindung zum Netzwerk besteht.

Wenn die Virenschutz- und Firewallsoftware auf manchen Computern, die nicht permanent mit dem Unternehmensnetzwerk verbunden sind, noch nicht installiert wurde, wird empfohlen, die Computer beim nächsten Zugriff auf das Netzwerk zu schützen. Anweisungen hierzu können Sie dem Abschnitt zum Schutz neuer Computer der Hilfe zu Sophos Control Center entnehmen.

## 5 Prüfen, ob Computer geschützt sind

Über das Dashboard können Sie prüfen, ob Ihre Computer im Netzwerk geschützt sind.

Das Dashboard bietet einen Überblick über den Sicherheitsstatus des Netzwerks. Sie können Grenzwerte festlegen, bei deren Erreichen auf dem Dashboard optische Warnungen angezeigt und Benachrichtigungen an die entsprechenden Computer gesendet werden.

Klicken Sie zum Anzeigen oder Ausblenden des Dashboards in der Symbolleiste auf die Schaltfläche **Dashboard**.

Die Konfiguration des Dashboards und die Symbole werden ausführlich in der *Hilfe* zu Sophos Control Center beschrieben.

## 6 Einrichten von E-Mail-Benachrichtigungen

Standardmäßig werden nur Desktop-Benachrichtigungen auf dem Computer angezeigt, auf dem der Threat gefunden wurde. Sie können Sophos Control Center so konfigurieren, dass bei Threat-Erkennung auch eine E-Mail-Benachrichtigung erfolgt.

So konfigurieren Sie E-Mail-Benachrichtigungen bei Threat-Erkennung:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** auf **Benachrichtigungen**.

Das Fenster **Benachrichtigung** wird angezeigt.

3. Klicken Sie auf der Registerkarte **E-Mail-Benachrichtigungen** auf die Option **E-Mail-Benachrichtigungen zulassen**, um E-Mail-Benachrichtigungen zu erhalten.
4. Wählen Sie unter **Bei folgenden Ereignissen eine Benachrichtigung senden**: die Ereignisse aus, zu denen jeweils eine E-Mail-Benachrichtigung gesendet werden soll.

**Hinweis:** Die Einstellungen zur Erkennung verdächtigen Verhaltens, Erkennung verdächtiger Dateien und zur Erkennung und Bereinigung von Adware und PUA gelten nur für Windows 2000 und aufwärts. Die Einstellung für sonstige Fehler trifft nur für Windows zu.

5. Sie können im Bereich **Empfänger** durch Klicken auf **Hinzufügen** oder **Entfernen** die E-Mail-Adressen bestimmen, an die Benachrichtigungen gesendet werden sollen. Klicken Sie auf **Umbenennen**, um die E-Mail-Adresse zu ändern, die Sie hinzugefügt haben.

**Hinweis:** Mac OS X-Computer senden Benachrichtigungen nur an den ersten Empfänger in der Liste.

6. Klicken Sie auf die Schaltfläche **SMTP konfigurieren**, um die Einstellungen für den SMTP-Server und die Sprache der E-Mail-Benachrichtigungen zu ändern.
7. Geben Sie in das Dialogfeld **SMTP-Einstellungen konfigurieren** Folgendes ein:
  - Geben Sie in das Textfeld **SMTP-Server** den Hostnamen oder die IP-Adresse des SMTP-Servers ein. Klicken Sie auf **Test**, um eine Test-E-Mail-Benachrichtigung zu senden.
  - Geben Sie in das Textfeld **SMTP-Absenderadresse** eine E-Mail-Adresse ein, an die nicht zustellbare Benachrichtigungen und Nicht-Zustellbarkeitsmeldungen gesendet werden sollen.
  - Im Textfeld **SMTP-Adresse für Rückantworten**: können Sie eine E-Mail-Adresse angeben, an die Antworten auf E-Mail-Benachrichtigungen gesendet werden können. E-Mail-Benachrichtigungen werden von einem Systemkonto gesendet.

**Hinweis:** Linux- und UNIX-Computer ignorieren „SMTP-Absender“- und „Rückantwort“-Adressen und verwenden die Adresse `root@<hostname>`.

  - Klicken Sie im Bereich **Sprache** auf den Drop-Down-Pfeil und wählen Sie die Sprache, in der die E-Mail-Benachrichtigungen gesendet werden sollen.

Sie können Sophos Control Center auch zum Versenden von E-Mail-Benachrichtigungen zum Netzwerkstatus auf der Basis des Schwellenwerts im Dashboard konfigurieren. Anweisungen zur Verwaltung der Benachrichtigungen finden Sie im entsprechenden Abschnitt in der *Hilfe* zu Sophos Control Center.

## 7 Scannen auf potenziell unerwünschte Anwendungen

Standardmäßig erkennt Sophos Anti-Virus Viren, Trojaner und Würmer. Sie können die Software auch zur Erkennung von Adware und potenziell unerwünschten Anwendungen (PUA) konfigurieren.

**Hinweis:** Diese Option beschränkt sich auf Sophos Anti-Virus unter Windows 2000 oder höher.

Es empfiehlt sich, die Suche nach potenziell unerwünschten Anwendungen über einen geplanten Scan zu starten. So wird der sichere Umgang mit Anwendungen gewährleistet, die bereits im Netzwerk laufen. Anschließend können Sie potenzielle unerwünschte Anwendungen von On-Access-Scans suchen lassen, damit Ihre Computer auch in Zukunft geschützt sind.

### 7.1 Durchführen eines geplanten Scans

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** unter **Geplante Scans** auf **Hinzufügen**, um einen neuen Scan zu erstellen. Wenn Sie einen Scan bearbeiten möchten, wählen Sie ihn aus der Liste aus und klicken Sie auf **Ändern**.
3. Klicken Sie im Dialogfenster **Geplanter Scan** auf **Konfigurieren** (im unteren Seitenbereich).
4. Klicken Sie im Dialogfeld **Einstellungen zu Scans und Bereinigung** auf die Registerkarte **Scans**. Aktivieren Sie im Feld **Scan-Optionen** die Option **Nach Adware und PUA scannen** und klicken Sie auf **OK**.

Unter Umständen erkennt und meldet Sophos Anti-Virus potenziell unerwünschte Anwendungen beim Scan. Sie können die Anwendungen zulassen oder von den Computern entfernen.

### 7.2 Zulassen von erwünschten Anwendungen

Sie können Anwendungen, die im Zuge eines geplanten Scans als Adware/PUA erkannt wurden, zulassen.

So können Sie Anwendungen zulassen:

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.
2. Klicken Sie im Fenster **Scans konfigurieren** auf **Autorisierungen**.
3. Führen Sie im Fenster **Authorization Manager** einen der folgenden Schritte durch:
  - Wählen Sie die zuzulassenden Anwendungen aus. Klicken Sie in der Liste der zugelassenen Anwendungen auf **Hinzufügen**.
  - Wenn eine Anwendung nicht angezeigt wird, klicken Sie auf **Neuer Eintrag**. Klicken Sie im nächsten Dialogfenster auf den Link zur Liste der potenziell unerwünschten Anwendungen von Sophos. Suchen Sie die Anwendung, die zugelassen werden soll, und geben Sie den Namen der Anwendung ins Feld **Name** ein.

## 7.3 Bereinigen von unerwünschten Anwendungen

Sie können Anwendungen, die im Zuge eines geplanten Scans als Adware/PUA erkannt wurden, bereinigen.

So bereinigen Sie eine Anwendung:

1. Klicken Sie links unter **Maßnahme** auf **Alerts und Fehler löschen**.

Das Dialogfeld **Alerts und Fehler löschen** wird angezeigt.

2. Deaktivieren Sie das Kontrollkästchen zu allen Anwendungen, die Sie entfernen möchten, oder klicken Sie auf **Alles markieren** und klicken Sie anschließend auf **Bereinigung**.

Dadurch werden alle bekannten Komponenten der gewählten Anwendungen von den gewählten Computern entfernt. Unter Umständen kann die Bereinigung einige Zeit in Anspruch nehmen.

**Hinweis:** Einige Anwendungen können nicht mit Sophos Control Center bereinigt werden. Wenn dies der Fall ist, gehen Sie zu dem betroffenen Computer und bereinigen Sie die Anwendung mit Sophos Anti-Virus.

Unter Umständen ist zur vollständigen Bereinigung von mehrkomponentigen Anwendungen ein Neustart erforderlich. Sollte dies der Fall sein, weist eine Meldung auf dem betroffenen Computer darauf hin, dass der Neustart des Computers sofort oder später erfolgen kann. Die Bereinigung wird erst nach dem Neustart des Computers vollständig abgeschlossen.

Wenn Sie sich auf der Sophos Website eingehender über eine bestimmte Anwendung informieren möchten, klicken Sie im Dialogfeld **Alerts und Fehler löschen** auf den Namen der Anwendung.

Wenn Sie auf **Löschen** klicken, werden die gewählten Anwendungen aus der Liste entfernt. Sie werden jedoch weder bereinigt noch zugelassen.

## 7.4 Aktivieren von On-Access-Scans auf Adware und potenziell unerwünschte Anwendungen

1. Klicken Sie links unter **Konfiguration** auf **Scans konfigurieren**.

Das Dialogfeld **Scans konfigurieren** wird angezeigt.

2. Klicken Sie auf **On-Access-Scans**.

Das Dialogfeld **On-Access-Scan-Einstellungen** wird angezeigt.

3. Aktivieren Sie im Feld **Scan-Optionen** die Option **Nach Adware und PUA scannen**. Klicken Sie auf **OK**.

Einige Anwendungen „überwachen“ Dateien und versuchen regelmäßig, auf sie zuzugreifen. Wenn die On-Access-Scans aktiviert sind, werden alle Zugriffe erkannt und mehrere Alerts ausgegeben.

## 8 Umgang mit Viren

So können Sie Viren bereinigen:

1. Klicken Sie in Sophos Control Center im **Dashboard** auf den Link **Viren/Spyware**.

Im Dialogfeld **Alerts und Fehler löschen** werden die betroffenen Computer sowie entsprechende Virendetails aufgelistet.

2. Wählen Sie die Viren aus, die bereinigt werden sollen, und klicken Sie auf **Bereinigung**.

Der Virus wird aus der betroffenen Datei bzw. dem betroffenen Bootsektor entfernt. Die Bereinigung macht allerdings keine Änderungen rückgängig, die der Virus bereits in dem Dokument verursacht hat, und sollte daher nur als vorübergehende Maßnahme eingesetzt werden. Ersetzen Sie die bereinigten Programme im Anschluss durch eine Kopie vom Original-Datenträger oder eine virenfreie Sicherungskopie. Unter Umständen kann die Bereinigung einige Zeit in Anspruch nehmen.

Einige Viren können nicht mit Sophos Control Center bereinigt werden. Wenn dies der Fall ist, gehen Sie zu dem betroffenen Computer und bereinigen Sie den Virus mit Sophos Anti-Virus.

Wenn mehrkomponentige Threats vorhanden sind, wird empfohlen, zunächst einen vollständigen geplanten Scan der Computer durchzuführen, um alle Threat-Komponenten zu ermitteln.

Wenn Sie sich auf der Sophos Website eingehender über einen bestimmten Virus informieren möchten, klicken Sie im Dialogfeld **Alerts und Fehler löschen** auf den Namen des Virus.

## 9 Einrichten der Firewall

Nach der Erstinstallation lässt Sophos Client Firewall zunächst unbedingt erforderlichen eingehenden und ausgehenden Datenverkehr zu.

**Hinweis:** Sophos Client Firewall unterstützt IPv6 nicht. Version 1 lässt IPv6-Pakete durch, die Versionen 1.5 und 2.0 blockieren oder erlauben alle IPv6-Pakete, je nach Konfiguration.

### 9.1 Konfigurieren der Firewall

Sie können die Firewall je nach Bedarf zum Zulassen oder Sperren von Datenverkehr konfigurieren. Standardmäßig lässt die Firewall unbedingt erforderlichen eingehenden und ausgehenden Datenverkehr zu.

So konfigurieren Sie die Firewall:

1. Klicken Sie links unter **Konfiguration** auf **Firewall konfigurieren**.
2. Klicken Sie im Firewall-Konfigurationsassistenten auf **Weiter**.
3. Wählen Sie auf der Seite **Firewall konfigurieren** eine der folgenden Optionen aus:
  - **Ein Standort**  
Wählen Sie diese Option für Computer, die immer an das Netzwerk angeschlossen sind, beispielsweise Desktop-Computer.
  - **Zwei Standorte**  
Diese Option bietet sich an, wenn die Firewall-Einstellungen in Abhängigkeit vom Computerstandort variieren sollen, z.B. im Büro (im Netzwerk) und extern. Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.
  - **Gesamten Verkehr zulassen**  
Bei Auswahl dieser Option wird die Firewall deaktiviert und der gesamte Firewall-Verkehr zugelassen.
4. Wenn Sie auf der vorherigen Seite **Zwei Standorte** gewählt haben, konfigurieren Sie auf der Seite **Netzwerkidentifizierung** DNS- bzw. Gateway-Erkennung des Netzwerks.

**Hinweis:** Die Seite **Netzwerkidentifizierung** wird nur bei Auswahl der Option **Zwei Standorte** angezeigt.

Sophos Control Center wendet unterschiedliche Einstellungen auf Computer an, je nachdem, ob Computer mit dem Netzwerk verbunden sind oder nicht.
5. Wählen Sie auf der Seite **Arbeitsmodus** einen Modus aus und geben Sie so an, wie die Firewall eingehenden und ausgehenden Datenverkehr behandeln soll.
  - **Eingehenden Datenfluss blockieren, ausgehenden Datenfluss erlauben**  
Bei Auswahl dieser Option wird unbedingt erforderlicher ausgehender Datenverkehr erlaubt, eingehender Verkehr jedoch gesperrt. Anwendungen werden in diesem Modus nicht erlaubt.

### ■ **Eingehenden und ausgehenden Datenfluss blockieren**

Bei Auswahl dieser Option sperrt die Firewall den gesamten ausgehenden Datenverkehr mit Ausnahme der von Ihnen angegebenen Anwendungen. Klicken Sie zum Hinzufügen von Anwendungen rechts neben der Option auf **Zulassen**. Zugelassene Anwendungen besitzen uneingeschränkten Netzwerkzugriff.

### ■ **Überwachen**

In diesem Modus werden festgelegte Regeln auf die Computer übertragen. Unbekanntem Datenverkehr wird der Zugriff auf das Netzwerk und das Internet gewährt. In diesem Modus werden Informationen an die Konsole übermittelt. In diesem Modus können Sie Informationen zum Netzwerk sammeln und geeignete Regeln erstellen.

### ■ **Benutzerdefiniert**

Durch Auswahl dieser Option können Sie die Konfiguration an Ihre Bedürfnisse anpassen. Klicken Sie auf **Erweitert**, um die erweiterte Firewall-Konfiguration aufzurufen.

**Hinweis:** Sie sollten nur Änderungen an den erweiterten Optionen vornehmen, wenn Sie wissen, wie sich dies auswirkt.

Weitere Informationen zur erweiterten Firewall-Konfiguration entnehmen Sie bitte der *Hilfe* zu *Sophos Endpoint Security and Control*.

6. Wählen Sie auf der Seite **Datei- und Druckerfreigabe** die Option **Datei- und Druckerfreigabe zulassen**, wenn Sie anderen Computern im Netzwerk den Zugriff auf Drucker und Freigaben auf dem Computer ermöglichen möchten.
7. Wenn Sie die Option **Zwei Standorte** ausgewählt haben, werden Sie zur Auswahl des Arbeitsmodus und der Datei- und Druckerfreigabe (wie in Schritt 5 und 6 erläutert) für den zweiten Standort (nicht im Netzwerk) aufgefordert.

Wenn Sie zu einem späteren Zeitpunkt Änderungen an den Einstellungen vornehmen möchten, können Sie den Assistenten erneut ausführen.

Nach der Konfiguration der Firewall können Sie Firewall-Ereignisse (z.B. von der Firewall gesperrte Anwendungen) in der **Firewall – Ereignisanzeige** aufrufen. Nähere Informationen entnehmen Sie bitte der *Hilfe* zu Sophos Control Center.

## 9.2 Umgang mit gesperrten Objekten

Unter Umständen sperrt Sophos Control Center Anwendungen oder Vorgänge, die Sie ausführen möchten. Verfahren Sie in diesem Fall wie folgt:

1. Klicken Sie in Sophos Control Center im **Dashboard** auf den Link **Firewall**.
2. Wählen Sie im Dialogfeld **Firewall – Ereignisanzeige** den Eintrag für die Anwendung aus, die Sie zulassen möchten oder für die Sie eine Regel erstellen möchten. Klicken Sie auf **Regel erstellen**.
3. Wählen Sie im Dialogfeld aus, ob Sie die Anwendung zulassen möchten oder eine Regel dafür erstellen möchten.

## 10 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](mailto: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.

## 11 Copyright

Copyright © 2011 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Marken von Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken 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.de](mailto:support@sophos.de) or via the web at <http://www.sophos.de/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™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source<sup>10</sup>, 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 us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

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 companies<sup>12</sup> 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 ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. 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 me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

### **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. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>

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

### **iMatix SFL**

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