

SOPHOS

simple + secure

Sophos Enterprise Manager Richtlinienanleitung

Produktversion: 4.7
Stand: Juli 2011



Inhalt

1	Einleitung.....	3
2	Allgemeine Empfehlungen.....	4
3	Einrichten einer Update-Richtlinie.....	5
4	Einrichten von Antivirus- und HIPS-Richtlinien.....	6
5	Einrichten von Firewall-Richtlinien.....	9
6	Einrichten von Device Control-Richtlinien.....	14
7	Einrichten von Manipulationsschutz-Richtlinien.....	16
8	Scan-Empfehlungen.....	18
9	On-Access-Scans.....	19
10	Geplante Scans.....	20
11	On-Demand-Scans	21
12	Ausschluss von Objekten von Scans.....	22
13	Technischer Support.....	23
14	Rechtlicher Hinweis.....	24

1 Einleitung

Diese Anleitung dient als Leitfaden zur Einrichtung von Richtlinien für Sophos Enterprise Manager-Software.

Insbesondere wird Folgendes beschrieben:

- Sinn und Zweck von Richtlinienempfehlungen
- Einrichtung und Implementierung von Richtlinien
- Scan-Optionen zur Erkennung von Objekten
- Bestimmung auszuschließender Objekte

Der Leitfaden richtet sich an:

- Benutzer von Enterprise Manager.
- Benutzer, die mehr über die Einrichtung und Implementierung von Richtlinien erfahren möchten.

Sie sollten die *Sophos Enterprise Manager Startup-Anleitung* bereits gelesen haben.

Die vollständige Enterprise Manager-Dokumentation steht auf http://www.sophos.de/support/docs/Enterprise_Manager-all.html zum Abruf bereit.

2 Allgemeine Empfehlungen

Bei der Installation von Enterprise Manager werden Standardrichtlinien erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Die Standardrichtlinien können lediglich eine allgemeine Schutzfunktion erfüllen. Wenn Sie Funktionen wie Device Control oder Manipulationsschutz nutzen möchten, müssen Sie neue Richtlinien erstellen oder die Standardrichtlinien entsprechend anpassen.

Hinweis: Sie können bis zu vier Richtlinien von jedem Typ erstellen.

Beim Einrichten von Richtlinien können folgende Tipps hilfreich sein:

- Übernehmen Sie in einer Richtlinie möglichst die Standardeinstellungen.
- Berücksichtigen Sie die Rolle des Computers (z.B. Desktop oder Server), wenn Sie die Richtlinienvoreinstellungen ändern oder neue Richtlinien erstellen.
- Konfigurieren Sie die Optionen und zentralen Richtlinieneinstellungen möglichst über Enterprise Manager statt auf dem Computer selbst.
- Optionen sollten auf einem Computer nur zur vorläufigen Konfiguration oder für Elemente geändert werden, die nicht zentral konfiguriert werden können, z.B. die erweiterten Scan-Optionen.
- Erstellen Sie für Computer mit besonderen Konfigurationsanforderungen eine separate Gruppe und Richtlinie.

3 Einrichten einer Update-Richtlinie

Die Update-Richtlinie legt fest, wie Computer neue Threat-Definitionen und Software-Updates erhalten. Durch Software-Abonnements wird festgelegt, welche Endpoint-Softwareversionen für die jeweiligen Plattformen von Sophos heruntergeladen werden. Die Standard-Update-Richtlinie ermöglicht Installation und Updates der Software, die im „empfohlenen“ Abonnement angegeben sind. Beim Einrichten von Update-Richtlinien können folgende Tipps hilfreich sein:

- Standardmäßig beziehen Computer von einer einzigen primären Quelle Updates. Es empfiehlt sich jedoch, stets eine Alternativ-Update-Quelle einzurichten. Wenn Endpoints keine Verbindung zur primären Quelle herstellen können, versuchen sie, Updates von der sekundären Quelle (falls vorhanden) zu beziehen. Weitere Informationen finden Sie in der Sophos Enterprise Manager Hilfe.
- Unter Umständen roamen Mitarbeiter mit Laptops sehr viel, auch international. In diesem Fall empfiehlt sich, Standort-Roaming in der Update-Richtlinie festzulegen. Wenn diese Option aktiviert ist, versuchen Laptops, den nächsten Standort aufzufinden und von dort upzudaten, indem Sie eine Anfrage an feste Endpoints in ihrem Netzwerk senden. Wenn mehrere Standorte gefunden werden, sucht das Laptop nach dem nächsten und greift auf diesen zu. Wenn dies nicht möglich ist, greift das Laptop auf den in der Update-Richtlinie festgelegten primären (und anschließend den sekundären) Standort zu. Standort-Roaming ist nur möglich, wenn der roamende Endpoint Updates von einer Quelle bezieht, die von der gleichen Instanz von Enterprise Manager verwaltet wird, die auch den Endpoint verwaltet. Weitere Informationen finden Sie in der Sophos Enterprise Manager Hilfe.
- Die Anzahl an Gruppen mit derselben Update-Richtlinie sollte überschaubar sein. Eine Update-Quelle sollte von nicht mehr als 1000 Computern beansprucht werden. Im Idealfall nutzen 600 bis 700 Computer dieselbe Update-Quelle.

Hinweis: Die Anzahl der Computer, die Updates über dieselbe Quelle beziehen können, hängt vom Update-Server und dem Netzwerk ab. In Enterprise Manager können Sie maximal vier neue Update-Richtlinien erstellen.

- Wenn Sie Leistungseinbußen befürchten, können Sie die Update-Frequenz von älteren Computermodellen jedoch auch verringern (so dass Updates zwei bis drei Mal täglich durchgeführt werden) oder einstellen, dass die Updates durchgeführt werden, wenn die Computer nicht genutzt werden (z.B. am Wochenende oder am Abend).



Vorsicht: Bedenken Sie, dass die Reduzierung der Update-Häufigkeit das Sicherheitsrisiko erhöht.

4 Einrichten von Antivirus- und HIPS-Richtlinien

4.1 Empfohlene Einstellungen

Die Antivirus- und HIPS-Richtlinie regelt die Erkennung und Bereinigung von Viren, Trojanern, Würmern, Spyware, Adware, potenziell unerwünschten Anwendungen, verdächtigem Verhalten und verdächtigen Dateien. Beim Einrichten der Antivirus- und HIPS-Richtlinie können folgende Tipps hilfreich sein:

- Die Antivirus- und HIPS-Standardrichtlinie schützt Computer vor Viren und sonstiger Malware. Sie können aber auch neue Richtlinien erstellen oder die Standardrichtlinie ändern, um die Erkennung anderer unerwünschter Anwendungen oder Verhaltensmuster zu ermöglichen.
- Nutzen Sie Sophos Live-Schutz: Über den Sophos Online-Abgleich-Dienst wird hierbei umgehend festgestellt, ob eine Datei eine Bedrohung darstellt und Sophos Software wird in Echtzeit upgedatet. Die Option **Live-Schutz aktivieren** ist standardmäßig aktiviert. Es empfiehlt sich ferner, die Option **Dateisamples automatisch an Sophos senden** zu aktivieren, um den Sophos Live-Schutz bestmöglich nutzen zu können.
- Wählen Sie die Option **Nur benachrichtigen**, um verdächtiges Verhalten nur zu erkennen. Definieren Sie zunächst eine Richtlinie im Benachrichtigungsmodus, um einen besseren Überblick über verdächtiges Verhalten im Netzwerk zu erhalten. Diese Option ist standardmäßig aktiviert und sollte nach der Richtlinienimplementierung deaktiviert werden, damit Programme und Dateien gesperrt werden können.

4.2 Implementieren einer Antivirus- und HIPS-Richtlinie

Verfahren Sie zum Implementieren der Antivirus- und HIPS-Richtlinie wie folgt:

1. Legen Sie am besten für jede Gruppe eine eigene Richtlinie an. In Enterprise Manager können Sie maximal vier neue Antivirus- und HIPS-Richtlinien erstellen.
2. Legen Sie Ausschlüsse von On-Access-Scans für Verzeichnisse oder Computer mit großen Datenbanken oder häufigen Änderungen unterliegenden Dateien fest. Stellen Sie sicher, dass diese Komponenten von On-Access-Scans erfasst werden. Es bietet sich beispielsweise unter Umständen an, bestimmte Verzeichnisse auf Exchange-Servern oder sonstigen Servern auszuschließen, um eventuellen Leistungseinbußen vorzubeugen. Weitere Informationen finden Sie im Sophos Support-Artikel 12421 (<http://www.sophos.de/support/knowledgebase/article/12421.html>).

3. Wählen Sie die gewünschten Optionen für Sophos Live-Schutz aus. Der Live-Schutz bietet dank des Online-Abgleich-Diensts sowie der Echtzeit-Software-Updates besonders aktuellen Schutz. Die folgenden Optionen sind vorhanden:

- **Live-Schutz aktivieren:** Wenn eine Datei von einem Antiviren-Scan auf einem Endpoint als verdächtig eingestuft wurde, anhand der Threatkennungsdateien (IDEs) auf dem Computer jedoch nicht festgestellt werden kann, ob die Datei virenfrei ist, werden bestimmte Daten (z.B. die Prüfsumme der Datei und weitere Attribute) zur weiteren Analyse an Sophos übermittelt. Durch einen Abgleich mit der Datenbank der Sophos Labs wird sofort festgestellt, ob es sich um eine verdächtige Datei handelt. Die Datei wird als virenfrei oder von Malware betroffen eingestuft. Das Ergebnis der Prüfung wird an den Computer übertragen, und der Status der Datei wird automatisch aktualisiert.

Diese Option ist standardmäßig aktiviert.

- **Dateisamples automatisch an Sophos senden:** Wenn die Datei als potenzielle Malware eingestuft wird, anhand der Eigenschaften der Datei jedoch keine eindeutige Klassifizierung möglich ist, kann Sophos über Sophos Live-Schutz ein Dateisample anfordern. Wenn die Option **Dateisamples automatisch an Sophos senden** aktiviert ist und Sophos noch kein Dateisample vorliegt, wird die Datei automatisch an Sophos übermittelt. Dateisamples helfen Sophos bei der Optimierung der Malware-Erkennung und minimieren falsche Erkennungen (sog. „False Positives“).

Wichtig: Sie müssen sicherstellen, dass die Sophos-Domäne, an die die Dateidaten gesendet werden, in Ihrer Web-Filter-Lösung zu den vertrauenswürdigen Seiten hinzugefügt wurde. Weitere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 62637 (<http://www.sophos.de/support/knowledgebase/article/62637.html>). Wenn Sie eine Web-Filter-Lösung von Sophos einsetzen (z.B. WS1000 Web Appliance), müssen Sie nicht tätig werden. Sophos-Domänen zählen zu den vertrauenswürdigen Seiten.

4. Aktivieren Sie die Erkennung von Viren und Spyware.
 - a) Aktivieren Sie On-Access-Scans oder planen Sie eine vollständige Systemüberprüfung ein, um Viren und Spyware zu erkennen. On-Access-Scans sind standardmäßig aktiviert. Mehr dazu erfahren Sie unter *On-Access-Scans* (Seite 19) und *Geplante Scans* (Seite 20).
 - b) Wählen Sie Bereinigungsoptionen für Viren/Spyware.
5. Die Erkennung verdächtiger Dateien lässt sich aktivieren.

Verdächtige Dateien weisen gewisse Malware-Merkmale auf, die jedoch nicht zur Einstufung der Dateien als neue Malware ausreichen.

 - a) Aktivieren Sie On-Access-Scans oder planen Sie eine vollständige Systemüberprüfung ein, um verdächtige Dateien zu erkennen.
 - b) Wählen Sie die Option **Verdächtige Dateien (HIPS)**.
 - c) Wählen Sie Bereinigungsoptionen für verdächtige Dateien.
 - d) Lassen Sie ggf. alle erlaubten Programme zu.
6. Aktivieren Sie die Erkennung verdächtigen Verhaltens und die Pufferüberlauf-Erkennung.

Im Rahmen der Erkennung von verdächtigem Verhalten und Pufferüberläufen werden laufende Prozesse ständig überwacht. So wird festgestellt, ob ein Programm verdächtiges

Verhalten zeigt. Diese Erkennungsmethoden eignen sich insbesondere zum Abwehren von Sicherheitsrisiken.

- a) Wählen Sie die Option **Nur benachrichtigen**, um nur verdächtiges Verhalten und Pufferüberläufe zu erkennen. Diese Option ist standardmäßig aktiviert.
- b) Lassen Sie Programme und Dateien zu, die Sie weiterhin verwenden möchten.
- c) Deaktivieren Sie die Option **Nur Alerts ausgeben**, wenn erkannte Programme und Dateien gesperrt werden sollen.

Dadurch wird das Sperren von Programmen und Dateien vermieden, die täglich genutzt werden. Weitere Informationen finden Sie im Sophos Support-Artikel 50160 (<http://www.sophos.de/support/knowledgebase/article/50160.html>).

7. Aktivieren Sie die Erkennung von Adware und PUA.

Wenn ein System zum ersten Mal auf Adware und PUA gescannt wird, können unzählige Alerts zu laufenden Anwendungen im Netzwerk ausgegeben werden. Wenn Sie zunächst einen geplanten Scan laufen lassen, können Sie die Anwendungen im Netzwerk sicher behandeln.

- a) Führen Sie eine vollständige Systemüberprüfung zur Erkennung von Adware und PUA durch.
- b) Lassen Sie vom Scan erkannte Anwendungen zu oder deinstallieren Sie sie.
- c) Wählen Sie die On-Access-Scan-Option **Adware und PUA** aus, um Adware und PUA zu erkennen.

Weitere Informationen finden Sie im Sophos Support-Artikel 13815 (<http://www.sophos.de/support/knowledgebase/article/13815.html>).

8. Die Erkennung von Threats in Webseiten kann aktiviert werden.

- a) Stellen Sie sicher, dass die Option **Zugriff auf schädliche Websites sperren** auf **Ein** steht, damit schädliche Websites gesperrt werden. Diese Option ist standardmäßig aktiviert.
- b) Wählen Sie für die Option **Download-Scans Ein** oder **Wie On-Access** aus, um heruntergeladene Daten zu scannen und zu sperren. Bei Auswahl der Option **Wie On-Access** (Standard) werden Download-Scans nur aktiviert, wenn auch On-Access-Scans aktiviert sind.
- c) Lassen Sie ggf. alle erlaubten Websites zu.

Weitere Informationen zum Einrichten der Antivirus- und HIPS-Richtlinie finden Sie in der Sophos Enterprise Manager Hilfe.

5 Einrichten von Firewall-Richtlinien

5.1 Informationen zur Firewall-Richtlinie

Die Firewall-Richtlinie regelt den Schutz der Netzwerkcomputer durch die Firewall. Nur genannten Anwendungen oder Anwendungsklassen wird der Zugriff auf das Unternehmensnetzwerk und das Internet gewährt.

Hinweis: Sophos Client Firewall wird auf Serverbetriebssystemen nicht unterstützt. Die Systemvoraussetzungen (Hardware und Software) entnehmen Sie bitte der Sophos Website: <http://www.sophos.de/products/all-sysreqs.html>.



Vorsicht: Firewall-Richtlinien müssen vor der Nutzung konfiguriert werden. Die Zuweisung einer unabgeänderten Standardrichtlinie mit Enterprise Manager zu einer Gruppe führt zu Problemen mit der Netzwerkkommunikation.

Die Standard-Firewall-Richtlinie ist nicht für die unabgeänderte Bereitstellung gedacht und eignet sich nicht für den normalen Gebrauch. Sie dient vielmehr als Basis zum Aufbau eigener Richtlinien.

Die Firewall ist standardmäßig aktiviert und blockiert alle unwichtigen Datenbewegungen. Bei Einsatz der Standard-Richtlinie, die nicht essenzielle Verbindungen blockiert, funktionieren nur wenige Programme. Daher sollten Sie bei der Konfiguration der Firewall alle Daten, Anwendungen und Prozesse festlegen, die nicht blockiert werden sollen. Testen Sie die Firewall vor der Installation und der Implementierung im gesamten Netzwerk.

5.2 Planen von Firewall-Richtlinien

Überlegen Sie sich vor dem Erstellen und Ändern von Firewall-Regeln (global, anwendungsbezogen oder Sonstiges), welche Aufgaben die Richtlinie erfüllen soll.

Es empfiehlt sich, folgende Aspekte beim Planen von Firewall-Richtlinien zu beachten:

- Auf welchen Computern soll Sophos Client Firewall installiert werden?
- Handelt es sich um Desktops oder Laptops? Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.
- Welche Standorterkennung soll verwendet werden (DNS-Suche bzw. Gateway-MAC-Adressenerkennung)?
- Netzwerkübergreifende Systeme und Protokolle.
- Remote-Verbindungen.

Je nach Anwendungen und Netzwerkzugriffsberechtigungen der unterschiedlichen Benutzergruppen können Sie entscheiden, wie viele Firewall-Richtlinien Sie erstellen müssen. Sie können maximal vier neue Firewall-Richtlinien erstellen. Die Richtlinien decken unterschiedliche Anwendungen ab und sind unterschiedlich restriktiv. Für mehrere Gruppen in Enterprise Manager müssen mehrere Richtlinien erstellt werden.

- Es wird davon abgeraten, nur eine Sophos Client Firewall-Richtlinie einzusetzen. Ansonsten müssen Sie Regeln für einen oder zwei Computer (beispielsweise die Arbeitsstation des

Administrators) übernehmen, die jedoch nicht im gesamten Netzwerk vorhanden sind. Die Sicherheit ist gefährdet.

- Im Umkehrschluss steigt bei zu vielen Konfigurationsoptionen der Überwachungs- und Wartungsaufwand.

Netzwerkübergreifende Systeme und Protokolle

Es gilt, Dienste im Netzwerk zu beachten. Beispiel:

- DHCP
- DNS
- RIP
- NTP
- GRE

Die meisten Dienste werden von Regeln der Standard-Firewall-Konfiguration abgedeckt. Beachten Sie Dienste, die zugelassen werden sollen und solche, die nicht benötigt werden.

Remote-Zugriff auf Computer

Wenn Computer per Remote-Zugriff überwacht oder gewartet werden, müssen Sie Regeln zur Remote-Software in die Konfiguration integrieren.

Ermitteln Sie Technologien für den Zugriff auf Computer im Netzwerk. Beispiel:

- RDP
- VPN Client/Server
- SSH/SCP
- Terminal Services
- Citrix

Überprüfen Sie, welche Zugriffsart erforderlich ist und passen Sie die Regeln entsprechend an.

5.3 Empfohlene Einstellungen

Beim Einrichten von Firewall-Richtlinien können folgende Tipps hilfreich sein:

- Bei der Installation von Sophos Client Firewall ist die Windows-Firewall deaktiviert. Wenn Sie also die Windows-Firewall genutzt haben, notieren Sie sich die Konfigurationen und übertragen Sie sie auf Sophos Client Firewall.
- Benutzen Sie den Modus **Standardmäßig zulassen**, um häufig auftretende Datenbewegungen, Anwendungen und Prozesse zu erkennen, jedoch nicht zu blockieren. Definieren Sie zunächst eine Richtlinie im Benachrichtigungsmodus, um einen besseren Überblick über die Datenbewegungen im Netzwerk zu erhalten.
- In der Firewall-Ereignisanzeige werden Datenbewegungen, Anwendungen und Prozesse festgehalten. Ferner lassen sich anhand der Ereignisanzeige Regeln zum Zulassen/Sperren

von erfassten Datenbewegungen, Anwendungen und Prozessen erstellen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Firewall-Ereignisse** aufrufen.

- Überprüfen Sie die erstellten Regeln in der Ereignisanzeige. Unter Umständen werden mehrere Firewall-Ereignisse zu einer Anwendung angezeigt. Eine Anwendungsregel muss jedoch alle Maßnahmen zu einer bestimmten Anwendung abdecken.
- Lassen Sie Webbrowser und E-Mail-Programme zu und geben Sie Dateien und Drucker zur gemeinsamen Nutzung frei.
- Wenn Sie sich nicht mit Netzwerken auskennen, raten wir von einer Änderung der voreingestellten ICMP-Einstellungen, globalen Regeln und Anwendungsregeln ab.
- Vermeiden Sie das Erstellen einer globalen Regel zugunsten einer Anwendungsregel, falls möglich.
- Bei der Auswahl von zwei Standorten kann der Modus **interaktiv** nicht in der Richtlinie festgelegt werden.
- Verwenden Sie den Modus **interaktiv** nicht bei mittelgroßen oder großen Netzwerken oder in Domänen-Umgebungen. Der Modus **interaktiv** bietet sich zur Erstellung von Firewall-Regeln für sehr kleine Netzwerke (beispielsweise bis zu 10 Computer) in Arbeitsgruppenumgebungen oder bei Einzelplatzrechnern an.

5.4 Einrichten der Firewall für zwei Standorte

Die einfache Standort-Option ist für Computer vorgesehen, die nur an ein einziges Netzwerk angebunden sind. Die Option für zwei Standorte ermöglicht unterschiedliche Firewall-Einstellungen an verschiedenen Standorten. Für Laptops empfiehlt sich die Auswahl mehrerer Standorte.

Folgendes ist bei der Einrichtung von zwei Standorten zu beachten:

- Legen Sie das von Ihnen kontrollierte Netzwerk (z.B. das Unternehmensnetz) als primären Standort fest und alle anderen Netzwerke als sekundären Standort.
- Der primäre Standort sollte im Allgemeinen weniger einschränkend sein als die sekundären Standorte.
- Beim Konfigurieren der Erkennungsoptionen für den primären Standort empfiehlt sich für umfangreiche Netzwerke die DNS-Erkennung, für einfache Netzwerke dagegen die Gateway-Erkennung. Für die DNS-Erkennung ist zwar ein DNS-Server erforderlich, doch diese Art der Erkennung ist in der Regel unkomplizierter als die Gateway-Erkennung. Wenn ein Gateway bei der Erkennung ausfällt, ist die erneute Konfiguration von MAC-Adressen erforderlich; außerdem könnte irrtümlich die Konfiguration für sekundäre Standorte bis zur Lösung des Hardware-Konfigurations-Problems übertragen werden.
- Bei der DNS-Erkennung empfiehlt sich das Anlegen eines speziellen DNS-Eintrags auf dem DNS-Server, der einen ungewöhnlichen Namen hat und eine Localhost-IP-Adresse (auch Loopback-Adresse genannt, z.B. 127.x.x.x) ausgibt. Diese Optionen schließen eine irrtümliche Erkennung eines anderen Netzwerks als primären Standort weitgehend aus.
- Wählen Sie im Bereich „Angewandter Standort“ der erweiterten Firewall-Richtlinie die zu übertragende Firewall-Richtlinie. Wenn die Konfiguration standortabhängig ist, wählen

Sie die Option **Konfiguration des erkannten Standorts**. Durch Auswahl der entsprechenden Option können Sie auch manuell eine Konfiguration auswählen.



Vorsicht: Bei lokalen Subnetzregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekanntem Subnetz her. Wenn dies der Fall ist, wird aufgrund der Firewallregeln der sekundären Konfiguration, bei denen die Adresse das lokale Subnetz ist, unter Umständen der gesamte unbekannte Datenverkehr zugelassen.

5.5 Implementieren einer Firewall-Richtlinie

Implementieren Sie eine Richtlinie zur Überwachung des Datenverkehrs im gesamten Netzwerk. In der Firewall-Ereignisanzeige können Sie Reports zum Datenverkehr abrufen. Erstellen Sie anhand dieser Daten eine Basisrichtlinie.

Sie sollten Sophos Client Firewall in Einzelschritten im Netzwerk verteilen, also Sophos Client Firewall Gruppe für Gruppe einzeln implementieren. So verhindern Sie in der Einführungsphase übermäßigen Datenfluss im Netzwerk.



Vorsicht: Implementieren Sie die Firewall erst dann im gesamten Netzwerk, wenn die Konfiguration eingehend getestet wurde.

1. Installieren Sie Sophos Client Firewall auf einer Testgruppe, in der die unterschiedlichen Rollen im Netzwerk vertreten sind.
2. Konfigurieren Sie eine Firewall-Richtlinie zur Verwendung des Modus **Standardmäßig zulassen**, um häufig auftretende Datenbewegungen, Anwendungen und Prozesse zu erkennen, jedoch nicht zu blockieren, und weisen Sie der Testgruppe die Richtlinie zu.
 - a) Erstellen Sie eine Firewall-Richtlinie. Rechtsklicken Sie in Enterprise Manager im Fenster **Richtlinien** auf **Firewall** und wählen Sie die Option **Richtlinie erstellen** aus. Geben Sie der Richtlinie einen Namen und doppelklicken Sie darauf.

Sie können jedoch auch die Standardrichtlinie ändern. Doppelklicken Sie im Bereich **Richtlinien** auf **Firewall** und dann auf **Standard**.

Der **Firewall-Richtlinienassistent** wird geöffnet.
 - b) Wenn Sie den Assistenten nutzen möchten, klicken Sie auf **Weiter**. Wenn Sie die Richtlinie manuell erstellen möchten, klicken Sie auf **Erweiterte Einstellungen der Firewall-Richtlinie**.
 - Im Assistenten: Klicken Sie auf **Weiter**. Wählen Sie **Ein Standort** und klicken Sie auf **Weiter**. Wählen Sie **Überwachen**, klicken Sie auf **Weiter**, erneut auf **Weiter** und anschließend auf **Fertig stellen**.
 - In den **Erweiterten Einstellungen** der Firewall: Klicken Sie im Dialogfeld **Firewall-Richtlinie** neben **Primärquelle** auf **Konfigurieren**. Wählen Sie auf der Registerkarte **Allgemein** den Arbeitsmodus **Standardmäßig zulassen**. Klicken Sie zwei Mal auf **OK**.
 - c) Weisen Sie der Testgruppe die neue Firewall-Richtlinie zu.

3. In der Firewall-Ereignisanzeige werden Datenbewegungen, Anwendungen und Prozesse festgehalten. Ferner lassen sich anhand der Ereignisanzeige Regeln zum Zulassen/Sperren von erfassten Datenbewegungen, Anwendungen und Prozessen erstellen. Sie können die Ereignisanzeige per Klick auf **Ansicht** > **Firewall-Ereignisse** aufrufen.
4. Es empfiehlt sich, die Firewall-Ereignisse über einen bestimmten Zeitraum hinweg (etwa einige Wochen lang) im Auge zu behalten und die Richtlinie daran anzupassen.
 - a) Erstellen Sie Regeln in der Ereignisanzeige. Rechtsklicken Sie auf ein Ereignis und erstellen Sie so eine Regel dafür. Nähere Informationen zur Erstellung von Firewall-Richtlinien finden Sie in der Sophos Enterprise Manager Hilfe unter „Konfigurieren von Richtlinien“ > „Konfigurieren von Firewall-Richtlinien“.
 - b) Untersuchen Sie die Richtlinie auf Schwachstellen (z.B. auf die Verteilung von Zugriffsrechten).
 - c) Bei unterschiedlichen Anforderungen unterteilen Sie die Gruppe und erstellen bei Bedarf weitere Richtlinien und Regeln.
5. Überprüfen Sie die erstellten Regeln in der Ereignisanzeige. Unter Umständen werden mehrere Firewall-Ereignisse zu einer Anwendung angezeigt. Eine Anwendungsregel muss jedoch alle Maßnahmen zu einer bestimmten Anwendung abdecken.
6. Teilen Sie das übrige Unternehmensnetzwerk in handhabbare Gruppen auf, in denen die diversen Rollen im Unternehmen vertreten sind (beispielsweise Computer der Vertriebsabteilung, der IT-Administratoren usw.). In Enterprise Manager können Sie maximal vier neue Firewall-Richtlinien erstellen.
7. Wenn Sie der Meinung sind, dass alle Bereiche abgedeckt wurden und nicht mehr viele neue Firewall-Ereignisse angezeigt werden, für die keine Regeln vorhanden sind, erstellen Sie Richtlinien anhand der Regeln und weisen Sie sie nach Bedarf zu. Bei einer großen Computeranzahl im Netzwerk empfiehlt sich, Sophos Client Firewall Gruppe für Gruppe einzeln zu installieren.
8. Wenn Sie die Regeln getestet haben, stellen Sie den Richtlinienmodus auf **Standardmäßig sperren** um.

Nähere Informationen zum Einrichten der Firewall-Richtlinie Sophos Enterprise Manager Hilfe unter „Konfigurieren von Richtlinien“ > „Konfigurieren von Firewall-Richtlinien“.

Hinweis: Als Alternative zur Überwachung des Datenverkehrs in der Firewall-Ereignisanzeige können Sie bei kleinen Netzwerken oder Einzelplatzrechnern Sophos Client Firewall auf einem Testcomputer installieren und im **interaktiven Modus** betreiben. Führen Sie so viele im Unternehmen genutzte Anwendungen (einschließlich Browsern) wie möglich aus. Importieren Sie dann die Firewall-Konfiguration und ändern Sie sie mit Regeln ab, die sich in diesem Prozess als nützlich erwiesen haben. Nähere Informationen entnehmen Sie bitte der Sophos Endpoint Security and Control Hilfe.

6 Einrichten von Device Control-Richtlinien

6.1 Empfohlene Einstellungen

Die Device Control-Richtlinie legt fest, welche Speicher- und Netzwerkgeräte verwendet werden dürfen. Beim Einrichten von Device Control-Richtlinien können folgende Tipps hilfreich sein:

- Bei Auswahl der Option **Geräte erkennen, aber nicht sperren** werden Controlled Devices zwar erkannt, jedoch nicht gesperrt. Hierzu müssen Sie zunächst den zu erkennenden Geräten den Status **Gesperrt** zuweisen. Die Software sucht nicht nach Gerätetypen, die nicht angegeben wurden. Definieren Sie zunächst eine „Report Only“-Richtlinie, um einen besseren Überblick über die Gerätenutzung im Netzwerk zu erhalten.
- Benutzen Sie die Device Control-Ereignisanzeige zur schnellen Filterung von Ereignissen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Device Control-Ereignisse** aufrufen.
- Mit dem Report Manager lassen sich Trendberichte zu Device Control-Ereignissen nach Computer oder Benutzer sortiert erstellen.
- Ziehen Sie eine strengere Zugriffssteuerung für Computer in Erwägung, deren Benutzer Zugriff auf vertrauliche Daten besitzen.
- Legen Sie bereits vor der Einführung einer Device Control-Richtlinie eine Liste von Geräten an, die nicht gesperrt werden sollen. So können Sie zum Beispiel optische Laufwerke für die DTP-Abteilung freigeben.
- Die Richtlinie „Secure Removable Storage“ kann zur automatischen Zulassung von hardwareseitig verschlüsselten USB-Speichermedien diverser Hersteller verwendet werden. Eine vollständige Liste unterstützter Hersteller steht auf der Sophos Website zum Abruf bereit. Eine vollständige Beschreibung der sicheren Wechselmedien ist dem Sophos Support-Artikel 63102 (<http://www.sophos.de/support/knowledgebase/article/63102.html>) zu entnehmen.
- Geben Sie beim Hinzufügen eines Geräteausschlusses zur Device Control-Richtlinie unter **Bemerkung** den Grund oder die zuständige Person für den Ausschluss ein.
- Anhand der benutzerdefinierten Desktop Messaging-Optionen können Sie Benutzern zusätzliche Hilfestellung bei der Erkennung eines Controlled Device leisten. Zum Beispiel können Sie einen Link zur Richtlinie zum Umgang mit Geräten Ihres Unternehmens angeben.
- Wenn der Computer nicht physisch mit dem Netzwerk verbunden ist und Sie ein Netzwerkgerät aktivieren möchten (z.B. einen WiFi-Adapter), wählen Sie beim Einstellen der Zugriffsstufen für Netzwerkgeräte die Option **Netzwerkbrücken sperren**.

Hinweis: Der Modus „Netzwerkbrücken sperren“ minimiert das Risiko von Netzwerkbrücken zwischen einem Unternehmensnetzwerk und einem unternehmensfremden Netzwerk. Der Modus „Netzwerkbrücken sperren“ steht für Wireless-Geräte und Modems zur Verfügung. Hierbei werden Wireless- oder Modemnetzwerkadapter deaktiviert, wenn ein Endpoint an ein physisches Netzwerk angeschlossen wird (in der Regel per Ethernet-Verbindung). Wenn der Endpoint von dem

physischen Netzwerk getrennt wird, wird der Wireless- oder Modemnetzwerkadapter wieder aktiviert.

- Überlegen Sie sich vor dem Einführen einer Richtlinie, welche Geräte gesperrt werden sollen. Berücksichtigen Sie alle möglichen Szenarien, besonders in Bezug auf Netzwerkverbindungen.



Vorsicht: Richtlinienänderungen werden über den Enterprise Manager-Server auf die entsprechenden Computer im Netzwerk übertragen. Wenn der Zugriff auf ein Netzwerk gesperrt ist, kann die Sperre nicht von Enterprise Manager aufgehoben werden, da keine Daten vom Server empfangen werden können.

6.2 Implementieren einer Device Control-Richtlinie

Device Control ist standardmäßig deaktiviert und alle Geräte sind zugelassen. Es empfiehlt sich folgender Umgang mit Device Control:

1. Überlegen Sie genau, welche Geräte gesteuert werden sollen.
2. Aktivieren Sie Device Control und wählen Sie die Option **Geräte erkennen, aber nicht sperren**, um Controlled Devices zu erkennen, jedoch nicht zu sperren. Hierzu müssen Sie zunächst den zu erkennenden Geräten den Status **Gesperrt** zuweisen. Die Software sucht nicht nach Gerätetypen, die nicht angegeben wurden.
Zunächst ist eine Device Control-Richtlinie vorhanden.
3. Aus der Ereignisanzeige zu Device Control ist ersichtlich, welche Geräte verwendet werden. Hier lässt sich auch bestimmen, welche Geräte bzw. Gerätetypen gesperrt werden sollen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Device Control-Ereignisse** aufrufen.
4. Wenn Sie den unterschiedlichen Computergruppen jeweils unterschiedliche Zugriffsrechte auf Geräte zuweisen möchten, erstellen Sie gruppenspezifische Richtlinien. So können Sie den Zugriff auf Wechselmedien zum Beispiel der IT- und Verkaufsabteilung gewähren, ihn jedoch für die Personal- und Finanzabteilung sperren. In Enterprise Manager können Sie maximal vier neue Device Control-Richtlinien erstellen.
5. Schließen Sie Instanzen und Modelltypen aus, die nicht gesperrt werden sollen. So können Sie z.B. einen bestimmten USB-Schlüssel (Instanz) oder alle Vodafone 3G-Modems (Modelltyp) ausschließen.
6. Ändern Sie den Status der Geräte, die gesperrt werden sollen, in **Gesperrt**. Manchen Speichergeräten können Sie zudem Lesezugriff zuweisen.
7. Konfigurieren Sie die Richtlinie so, dass Controlled Devices gesperrt werden: Deaktivieren Sie hierzu die Option **Geräte erkennen, aber nicht sperren**.

Auf diese Weise verhindern Sie eine übermäßige Erzeugung von Alerts und die Sperrung von Geräten, die von einigen Benutzern evtl. noch benötigt werden. Nähere Informationen zum Einrichten der Device Control-Richtlinie entnehmen Sie bitte der Sophos Enterprise Manager Hilfe.

7 Einrichten von Manipulationsschutz-Richtlinien

7.1 Empfohlene Einstellungen

Mit der Manipulationsschutz-Richtlinie können Sie verhindern, dass Benutzer (lokale Administratoren ohne hinreichende Fachkenntnisse) Sophos Sicherheitssoftware umkonfigurieren, deinstallieren oder deaktivieren. Benutzer ohne Manipulationsschutzkennwort können diese Aufgaben nicht durchführen.

Hinweis: Der Manipulationsschutz schützt nicht vor Benutzern mit ausgeprägtem Technikverständnis. Auch bietet die Funktion keinen Schutz vor Malware, die eigens dafür konzipiert wurde, das Betriebssystem zu untergraben und die Erkennung zu umgehen. Diese Malware-Art wird ausschließlich von Scans auf Threats und verdächtigem Verhalten erkannt. Weitere Informationen finden Sie unter [Einrichten von Antivirus- und HIPS-Richtlinien](#) (Seite 6).

Nach der Aktivierung des Manipulationsschutzes und der Erstellung eines Manipulationsschutzkennworts können Benutzer, die das Kennwort nicht kennen, keine Änderungen an der Konfiguration von On-Access-Scans oder der Erkennung verdächtigen Verhaltens in Sophos Endpoint Security and Control vornehmen, den Manipulationsschutz nicht deaktivieren und keine Komponenten von Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System) oder Sophos SafeGuard Disk Encryption über die Systemsteuerung deaktivieren.

Beim Einrichten der Manipulationsschutz-Richtlinien können folgende Tipps hilfreich sein:

- Die Ereignisanzeige des Manipulationsschutzes gibt Aufschluss über den Gebrauch des Manipulationsschutzkennworts und die unternommenen Manipulationsversuche im Unternehmen. Es werden erfolgreiche Manipulationsschutz-Authentifizierungsversuche (autorisierte Benutzer umgehen den Manipulationsschutz) und nicht erfolgreiche Versuche, Sophos Sicherheitssoftware zu manipulieren, angezeigt. Sie können die Ereignisanzeige per Klick auf **Ansicht > Manipulationsschutz-Ereignisse** aufrufen.

7.2 Implementieren der Manipulationsschutz-Richtlinie

Standardmäßig ist der Manipulationsschutz deaktiviert. Folgende Empfehlungen können beim Einrichten des Manipulationsschutzes hilfreich sein:

1. Aktivieren Sie den Manipulationsschutz und erstellen Sie ein sicheres Manipulationsschutzkennwort.

Mit diesem Kennwort können nur autorisierte Benutzer Sophos Sicherheitssoftware konfigurieren, deaktivieren oder deinstallieren.

Hinweis: Der Manipulationsschutz betrifft Mitglieder der Gruppe SophosUsers und SophosPowerUsers nicht. Auch bei aktiviertem Manipulationsschutz können diese Benutzer weiterhin ohne Eingabe von Kennwörtern die Aufgaben ausführen, zu deren Ausführung sie berechtigt sind.

2. Wenn Sie den Manipulationsschutz deaktivieren oder unterschiedliche Kennwörter für unterschiedliche Gruppen erstellen möchten, erstellen Sie unterschiedliche Richtlinien für die jeweiligen Gruppen. In Enterprise Manager können Sie maximal vier neue Manipulationsschutz-Richtlinien erstellen.

Nähere Informationen zum Einrichten der Manipulationsschutz-Richtlinie entnehmen Sie bitte der Sophos Enterprise Manager Hilfe.

8 Scan-Empfehlungen

Die in den folgenden Abschnitten ausgeführten Scan-Optionen werden in der Antivirus- und HIPS-Richtlinie festgelegt. Beim Einrichten der Scan-Optionen können folgende Tipps hilfreich sein:

- Verwenden Sie möglichst die Voreinstellungen.
- Konfigurieren Sie Scans möglichst mit Enterprise Manager statt auf dem Computer.
- Berücksichtigen Sie die Rolle des Computers (z.B. Desktop oder Server).

Erweiterungen

Wenn Sie die Erweiterungsoptionen für On-Access-Scans öffnen möchten, klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Konfigurieren** neben **Aktivieren von On-Access-Scans** und rufen Sie anschließend die Registerkarte **Erweiterungen** auf.

Bei geplanten Scans klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** auf **Erweiterungen und Ausschlüsse**.

- Die Option **Alle Dateien scannen** empfiehlt sich im Allgemeinen nicht. Wählen Sie stattdessen die Option **Nur ausführbare und anfällige Dateien scannen**, um Threats zu erfassen, die von den SophosLabs registriert wurden. Die Option zum Scannen aller Dateien sollte nur auf Anweisung des technischen Supports verwendet werden.

Sonstige Scan-Optionen

Wenn Sie die sonstigen Scan-Optionen für On-Access-Scans öffnen möchten, klicken Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** auf **Konfigurieren** neben **Aktivieren von On-Access-Scans**.

Bei geplanten Scans wählen Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** im Bereich **Geplante Scans** einen Scan aus und klicken auf **Bearbeiten**. Klicken Sie dann im Dialogfeld **Einstellungen zu geplanten Scans** auf **Konfigurieren**.

- Die Option **Archivdateien scannen** bremst die Scangeschwindigkeit ab und wird selten benötigt. Wenn Sie eine Archivdatei öffnen, um den Inhalt abzurufen, wird die Datei automatisch gescannt. Wenn Sie nicht regelmäßig mit Archivdateien arbeiten, raten wir von dieser Option ab.
- Es empfiehlt sich, den Systemspeicher auf Threats zu scannen. Der Systemspeicher wird vom Betriebssystem genutzt. Sie können den Systemspeicher regelmäßig bei aktivierten On-Access-Scans im Hintergrund scannen lassen. Sie können den Systemspeicher auch im Rahmen eines geplanten Scans scannen. **Systemspeicher-Scans** sind standardmäßig aktiviert.

9 On-Access-Scans

Für On-Access-Scans gelten folgende Empfehlungen:

- Verwenden Sie möglichst die Voreinstellungen.
- Wählen Sie die On-Access-Scan-Option **Beim Lesen**. Die On-Access-Scan-Optionen **Beim Schreiben** und **Beim Umbenennen** sind lediglich zur Erhöhung der Sicherheit vorgesehen und werden selten benötigt. Sie empfehlen sich jedoch bei Malwareausbrüchen.
- Einige Verschlüsselungsprogramme verhindern die Virenerkennung durch On-Access-Scans. Passen Sie die automatisch gestarteten Prozesse so an, dass Dateien bereits vor On-Access-Scans entschlüsselt werden. Weitere Informationen zum Einsatz der Antivirus- und HIPS-Richtlinie in Kombination mit Verschlüsselungssoftware entnehmen Sie bitte dem Sophos Support-Artikel 12790
<http://www.sophos.de/support/knowledgebase/article/12790.html>.
- Wenn Sie On-Access-Scans nicht benötigen, sollten zumindest geplante Scans eingerichtet werden. Weitere Informationen finden Sie unter *Geplante Scans* (Seite 20).



Vorsicht: Bedenken Sie, dass die Deaktivierung von On-Access-Scans ein höheres Sicherheitsrisiko mit sich bringt.

10 Geplante Scans

Für geplante Scans gelten folgende Empfehlungen:

- Verwenden Sie möglichst die Voreinstellungen.
- Mit geplanten Scans können Sie Threats und das Aufkommen unerwünschter Anwendungen besser einschätzen.
- Geplante Scans empfehlen sich für Serververzeichnisse, deren Zugriffsgeschwindigkeit ansonsten durch die langsameren On-Access-Scans beeinträchtigt werden kann. So können z.B. für eine Gruppe von Exchange-Servern zeitgeplante Scans für bestimmte Verzeichnisse eingerichtet werden. Weitere Informationen finden Sie im Sophos Support-Artikel 12421 (<http://www.sophos.de/support/knowledgebase/article/12421.html>).
- Wenn Sie On-Access-Scans nicht benötigen, sollten zumindest geplante Scans eingerichtet werden. Gruppieren Sie diese Computer und definieren Sie einen geplanten Scan.
- Berücksichtigen Sie beim Planen eines Scans Belastungsspitzen. Wenn z.B. ein Server gescannt werden soll, der ständig auf Datenbanken zugreift, planen Sie einen Zeitpunkt für geplante Scans ein, an dem sie den Betrieb am wenigsten beeinträchtigen.
- Bedenken Sie im Falle eines Servers auch die gerade ausgeführten Tasks. Während eines Backups sollte nicht gleichzeitig ein geplanter Scan ausgeführt werden.
- Scans sollten zu bestimmten Zeiten ausgeführt werden. Auf allen Computern sollte täglich ein geplanter Scan ausgeführt werden. Zumindest einmal pro Woche sollte ein geplanter Scan auf allen Computern anstehen.
- Unter Windows Vista und höher können Sie einen geplanten **Scan mit niedriger Priorität** ausführen, um die Auswirkungen auf Anwendungen zu minimieren. Die Option empfiehlt sich, erhöht jedoch die Scan-Dauer.

11 On-Demand-Scans

On-Demand-Scans empfehlen sich unter folgenden Umständen:

- Auf einem System ist eine manuelle Prüfung oder Bereinigung erforderlich.

12 Ausschluss von Objekten von Scans

So verhindern Sie, dass bestimmte Objekte gescannt werden:

- Geben Sie Erweiterungen an, um bestimmte Dateitypen von Scans auszuschließen.
- Durch Ausschlüsse können Sie bestimmte Objekte, wie Dateien oder Laufwerke, von Scans ausschließen. Ausschlüsse lassen sich auf Basis von Laufwerken (X:), Verzeichnissen (X:\Programme\Exchsrvr\) und Dateien (X:\Programme\SomeApp\SomeApp.exe) angeben.
- Es bietet sich an, Wechselmedien für Benutzer, die auf die Verwendung solcher Medien angewiesen sind, von On-Access-Scans auszuschließen. Da Medienlaufwerke über Lese- und Schreibvorgänge auf temporäre Dateien zugreifen, wird jede Datei beim Zugriff vom On-Access-Scanner erfasst und die Scan-Geschwindigkeit abgebremst.
- Mit der Option **Remote-Dateien ausschließen** können Sie Dateien, die sich an anderen Orten im Netzwerk befinden, von Scans ausschließen. Grundsätzlich sollten Remote-Dateien beim Zugriff gescannt werden. Das Ausschließen empfiehlt sich jedoch auf Dateiservern oder auch für große und/oder häufig geänderte Remote-Dateien.



Vorsicht: Bedenken Sie, dass das Ausschließen von Objekten ein höheres Sicherheitsrisiko mit sich bringt.

13 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.

14 Rechtlicher Hinweis

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.

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 us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

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 companies¹² 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 ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. 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 me²¹ know.

Douglas C. Schmidt²²

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
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/>

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>.

Common Public License

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>

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.

iMatix SFL

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

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. Alle Rechte vorbehalten.

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 (ey@cryptsoft.com).

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

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (ey@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.]