

Sophos Endpoint Security and Control 9.7 Richtlinienanleitung

Stand: April 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 Application Control-Richtlinien.....	13
7	Einrichten von Device Control-Richtlinien.....	15
8	Einrichten von Data Control-Richtlinien.....	17
9	Einrichten der Manipulationsschutz-Richtlinien.....	22
10	Einrichten von NAC-Richtlinien.....	24
11	Scan-Empfehlungen.....	26
12	On-Access-Scans.....	27
13	Geplante Scans.....	28
14	On-Demand-Scans	29
15	Ausschluss von Objekten von Scans.....	30
16	Technischer Support.....	31
17	Rechtlicher Hinweis.....	32

1 Einleitung

Diese Anleitung dient als Leitfaden zur Einrichtung von Richtlinien für Sophos Endpoint Security and Control-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 Console.
- Benutzer, die mehr über die Einrichtung und Implementierung von Richtlinien erfahren möchten.

Sie sollten die *Sophos Endpoint Security and Control Schnellstartanleitung* bereits gelesen haben.

Die vollständige Enterprise Console -Dokumentation steht auf www.sophos.de/support/docs/Enterprise_Console-all.html zum Abruf bereit.

2 Allgemeine Empfehlungen

Bei der Installation von Enterprise Console werden Standardrichtlinien erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Die Standardrichtlinien können lediglich eine allgemeine Schutzfunktion erfüllen. Wenn Sie Funktionen wie Application Control, Device Control, Data Control, Manipulationsschutz oder Network Access Control (NAC) nutzen möchten, müssen Sie neue Richtlinien erstellen oder die Standardrichtlinien entsprechend anpassen. 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 Console statt auf dem Computer selbst.
- Optionen sollten auf einem Computer nur zur vorläufigen Konfiguration oder für Objekte 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:

- In der Regel bietet sich die „empfohlene“ Version an. So wird Software automatisch auf dem neuesten Stand gehalten. Wenn Sie jedoch neue Versionen der Software vor der Bereitstellung im Netzwerk evaluieren möchten, empfiehlt sich die vorübergehende Verwendung von festen Softwareversionen im Hauptnetzwerk. Feste Versionen werden mit neuen Threat-Erkennungsdaten, jedoch nicht mit den monatlichen Software-Updates upgedatet.
- 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.

- 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 Hilfe zu Sophos Enterprise Console.
- 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 Updates, 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 mit Sophos Update Manager möglich. Als Voraussetzung muss der roamende Endpoint Updates von einer Quelle beziehen, die von der gleichen Instanz von Enterprise Console verwaltet wird, die auch den Endpoint verwaltet. Weitere Informationen finden Sie in der Hilfe zu Sophos Enterprise Console.
- Wenn Sie Leistungseinbußen bei älteren Computermodellen befürchten, können Sie eine feste Version der Software abonnieren und das Abonnement manuell ändern, wenn Sie bereit zum Updaten der Software der Computer sind. Durch Auswahl dieser Option wird sichergestellt, dass die Computer mit den aktuellen Threat-Erkennungsdaten upgedatet werden. Sie können 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.
- Aktivieren 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 nur bei neuen Softwareinstallationen standardmäßig aktiviert. Bei Software-Upgrades muss diese Option aktiviert werden. 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 „Report Only“-Richtlinie, 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.
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.

Die Option ist nur bei neuen Softwareinstallationen standardmäßig aktiviert. Bei Software-Upgrades muss diese Option aktiviert werden.

- **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 27) und *Geplante Scans* (Seite 28).
 - 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 Console zu Hilfe.

5 Einrichten von Firewall-Richtlinien

5.1 Empfohlene Einstellungen

Die Firewall-Richtlinie regelt den Schutz der Netzwerkcomputer durch die Firewall. Beim Einrichten von Firewall-Richtlinien können folgende Tipps hilfreich sein:

- Nach der Installation von Sophos Client Firewall wird die Windows-Firewall deaktiviert. Notieren Sie sich daher Systeme, die zuvor von der Windows-Firewall geschützt wurden, und stellen Sie diese Systeme auf Sophos Client Firewall um.
- Benutzen Sie den Modus **Standardmäßig zulassen**, um häufig auftretende Datenbewegungen, Anwendungen und Prozesse zu erkennen, jedoch nicht zu blockieren. Definieren Sie zunächst eine „Report Only“-Richtlinie, 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.
- Aktivieren Sie auf Testcomputern den Modus **Interaktiv** zum Testen von Lerndialogen, Erkennen und Konfigurieren von täglich eingesetzten Anwendungen und zum Importieren/Anpassen von Regeln.
- Im Modus **Interaktiv** empfiehlt es sich, die Option **Alert in Management-Konsole anzeigen, wenn Anwendungsregel lokal geändert wird** zu deaktivieren. So lässt sich bei der Reaktion auf Lerndialoge die Warnmeldung „Abweichend von Richtlinie“ unterdrücken.
- 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.

5.2 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 unbekanntete Datenverkehr zugelassen.

5.3 Sperren/Zulassen von Datenverkehr, Anwendungen und Prozessen

Beim Sperren und Zulassen von Datenverkehr, Anwendungen und Prozessen sollte Folgendes beachtet werden:

- Wenn die Firewall im **interaktiven** Modus läuft, teilen Sie den Benutzern mit, welche Daten, Anwendungen bzw. Prozesse gesperrt werden sollen und welche zugelassen werden dürfen.
- Wenn die Firewall im Modus **Standardmäßig sperren** läuft, werden keine Lerndialoge angezeigt. Das Sperren und Zulassen von Datenverkehr, Anwendungen und Prozessen erfolgt durch den Administrator über Enterprise Console.
- Die Optionen **...dieses Mal sperren** sollten nur in Zweifelsfällen verwendet werden. Diese Optionen stehen nur zur Verfügung, wenn sich die Richtlinie im **interaktiven** Modus befindet.
- In bestimmten Fällen sollte der Datenverkehr **nicht** gesperrt werden. Dazu gehören die Prüfsumme und die Anwendungsregeln in Bezug auf Webbrowser, E-Mail-Anwendungen, Datei- und Druckerfreigabe und andere Programme, die Internetzugang benötigen.
- Wenn ein Computer mit den zugelassenen Anwendungen eingerichtet wird, sollten Abfragen nur bei neuen Installationen oder beim Patchen vorhandener Anwendungen (im **interaktiven** Modus) angezeigt werden.

5.4 Implementieren einer Firewall-Richtlinie

Die Firewall ist standardmäßig aktiviert und blockiert alle unwichtigen Datenbewegungen. 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. Folgende Empfehlungen können beim Einrichten der Firewall-Richtlinie hilfreich sein:

1. Überlegen Sie sich vor dem Erstellen und Ändern von Firewall-Regeln, welche Aufgaben die Richtlinie erfüllen soll.
2. Benutzen Sie den Modus **Standardmäßig zulassen**, um häufig auftretende Datenbewegungen, Anwendungen und Prozesse zu erkennen, jedoch nicht zu blockieren.
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. Erstellen Sie je nach Bedarf Ihre individuellen globalen Regeln und Anwendungsregeln.

Hinweis: Sie können auch einen Testcomputer im **interaktiven** Modus konfigurieren und die dadurch erfassten Regeln importieren und an Ihre Bedürfnisse anpassen. In diesem Fall ignorieren Sie bitte die bisherigen vier Schritte. Weitere Informationen finden Sie in der Hilfe zu Sophos Endpoint Security and Control.

5. Implementieren Sie die Firewall schrittweise im Netzwerk. So verhindern Sie in der Einführungsphase übermäßigen Datenfluss im Netzwerk. Installieren Sie die Firewall zunächst nur auf einer überschaubaren Anzahl von Computern. Die Computer sollten jedoch aus verschiedenen Gruppen gewählt werden, die unterschiedliche Rollen erfüllen.



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

- a) Installieren und konfigurieren Sie Sophos Client Firewall auf Test-Computern.
 - b) Starten Sie auf den Computern alle gewohnten Programme und Prozesse.
 - c) Untersuchen Sie die Testkonfiguration auf Schwachstellen (z.B. auf die Verteilung von Zugriffsrechten).
 - d) Bei unterschiedlichen Anforderungen unterteilen Sie die Gruppe und konfigurieren sie entsprechend.
 - e) Wenn Sie die Regeln getestet haben, stellen Sie den Richtlinienmodus auf **Standardmäßig sperren** um.
6. Wenn die erste Phase der Einführung abgeschlossen ist, bereiten Sie die Implementierung der Firewall im gesamten Netzwerk vor.
Vermeiden Sie übermäßige Datenbewegungen im Netzwerk. Führen Sie die Implementierung in mehreren Schritten durch.

- Teilen Sie das Netzwerk in überschaubare Gruppen auf (die z.B. nicht mehr als 100 Computer umfassen).
- Installieren Sie die Firewall nach und nach in diesen Gruppen.

Weitere Informationen zum Einrichten der Firewall-Richtlinie finden Sie in der Hilfe zu Sophos Enterprise Console. Weitere Informationen zu den Voreinstellungen der Firewall finden Sie im Sophos Support-Artikel 14464 (<http://www.sophos.de/support/knowledgebase/article/14464.html>).

Die neuen Firewall-Funktionen in Enterprise Console 4.0 werden im Sophos Support-Artikel 54750 (<http://www.sophos.de/support/knowledgebase/article/54750.html>) beschrieben.

6 Einrichten von Application Control-Richtlinien

6.1 Empfohlene Einstellungen

Über die Application Control-Richtlinie wird der Zugriff auf Anwendungen im Netzwerk geregelt, d.h. Anwendungen werden entweder gesperrt oder zugelassen. Solche Anwendungen werden als Controlled Applications bezeichnet. Beim Einrichten von Application Control-Richtlinien können folgende Tipps hilfreich sein:

- Bei Aktivieren der Option **Erkennen, aber laufen lassen** werden Controlled Applications zwar erkannt, jedoch nicht gesperrt. Definieren Sie zunächst eine „Report Only“-Richtlinie, um einen besseren Überblick über die Nutzung von Anwendungen im Netzwerk zu erhalten.
- Über die Ereignisanzeige zu Application Control lässt sich die Nutzung von Anwendungen in Ihrem Unternehmen prüfen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Application Control-Ereignisse** aufrufen.
- Mit dem Report Manager lassen sich Trendberichte zu Application Control-Ereignissen nach Computer oder Benutzer sortiert erstellen.
- Nutzen Sie die Option „Neue Anwendungen“, um neue, von Sophos ermittelte Anwendungen eines bestimmten Typs zu sperren. Auf diese Weise müssen Sie nicht ständig die Richtlinie ändern. Wenn Sie zum Beispiel alle Instant-Messaging-Anwendungen sperren, empfiehlt es sich, alle neuen Anwendungen dieses Typs zu sperren.

6.2 Implementieren einer Application Control-Richtlinie

Standardmäßig werden alle Anwendungen und Anwendungstypen zugelassen. Es empfiehlt sich folgender Umgang mit Application Control:

1. Überlegen Sie genau, welche Anwendungen gesteuert werden sollen.
2. Aktivieren Sie On-Access-Scans und wählen Sie die Option **Erkennen, aber laufen lassen**, um Controlled Applications zwar zu erkennen, jedoch nicht zu sperren.
Zunächst ist eine Application Control-Richtlinie vorhanden.
3. Aus der Ereignisanzeige zu Application Control ist ersichtlich, welche Anwendungen verwendet werden. Hier lässt sich auch bestimmen, welche Anwendungen bzw. Anwendungstypen gesperrt werden sollen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Application Control-Ereignisse** aufrufen.
4. Wenn Sie den unterschiedlichen Computergruppen jeweils unterschiedliche Zugriffsrechte auf Anwendungen zuweisen möchten, erstellen Sie gruppenspezifische Richtlinien. So kann beispielsweise VoIP im Büro unterbunden, auf Remote-Computern jedoch zugelassen werden.
5. Bestimmen Sie, welche Anwendungen oder Anwendungsarten Sie blockieren möchten und verschieben Sie sie in die Liste der blockierten Anwendungen.
6. Konfigurieren Sie die Richtlinie so, dass Controlled Applications gesperrt werden: Deaktivieren Sie hierzu die Option **Erkennen, aber laufen lassen**.

Durch das Befolgen dieser Schritte umgehen Sie das Problem, dass zahlreiche Alerts ausgelöst und wichtige Anwendungen gesperrt werden. Weitere Informationen zum Einrichten einer Application Control-Richtlinie finden Sie in der Hilfe zu Sophos Enterprise Console.

7 Einrichten von Device Control-Richtlinien

7.1 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 geben. 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 Console-Server auf die entsprechenden Computer im Netzwerk übertragen. Wenn der Zugriff auf ein Netzwerk gesperrt ist, kann die Sperre nicht von Enterprise Console aufgehoben werden, da keine Daten vom Server empfangen werden können.

7.2 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 der Finanzabteilung sperren.
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. Weitere Informationen zum Einrichten der Device Control-Richtlinie finden Sie in der Hilfe zu Sophos Enterprise Console.

8 Einrichten von Data Control-Richtlinien

8.1 Definieren der Data Control-Richtlinie

Mit der Data Control-Richtlinie können Sie die mit der versehentlichen Übertragung vertraulicher Daten verbundenen Risiken eindämmen.

Jedes Unternehmen definiert „vertrauliche Daten“ auf seine eigene Weise. Einige Beispiele:

- Kundendaten
- Finanzdaten (z.B. Kreditkartennummern)
- Vertrauliche Dokumente

Wenn die Data Control-Richtlinie aktiviert ist, überwacht Sophos die Benutzeraktionen an Datenaustrittspunkten:

- Übertragungen von Dateien auf Speichermedien (Wechselspeicher, optische Speicher und Festplatten)
- Hochladen von Dateien in Anwendungen (Webbrowser, E-Mail-Clients und Instant-Messaging-Clients)

Eine Data Control-Regel besteht aus drei Elementen:

- Aufzufindende Objekte: Dateiinhalt, Dateitypen, Dateinamen etc.
- Zu überwachende Objekte: z.B. Speichertypen und Anwendungen
- Zu ergreifende Maßnahmen: Dazu zählen „Dateiübertragung zulassen und Ereignis protokollieren“ (Überwachungsmodus), „Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren“ (Lernmodus) und „Übertragung sperren und Ereignis protokollieren“ (Einschränkungsmodus)

So können Sie z.B. eine Data Control-Regel zur Protokollierung des Hochladens einer Tabelle über Internet Explorer definieren. Oder Sie definieren eine Regel, die das Kopieren von Kundenadressen auf eine DVD ermöglicht, wenn der Benutzer dies bestätigt.

Die Definition vertraulicher Daten auf Inhaltsbasis gestaltet sich etwas schwieriger. In sog. Content Control Lists hat Sophos Definitionen vertraulicher Daten zusammengestellt, die diese Aufgabe vereinfachen. Diese Listen enthalten eine breitgefächerte Auswahl personenbezogener und finanzieller Datenformate und werden regelmäßig von Sophos ergänzt. Bei Bedarf können Sie auch eigene Content Control Lists erstellen.

Die Data Control-Richtlinie wird auch auf Computern durchgesetzt, die nicht ständig mit dem Unternehmensnetzwerk verbunden sind.

8.2 Empfohlene Einstellungen

Beim Einrichten von Data Control-Richtlinien können folgende Tipps hilfreich sein:

- Bei Auswahl der Option **Dateiübertragung zulassen und Ereignis protokollieren** werden Daten erkannt, jedoch nicht gesperrt. Definieren Sie zunächst eine „Report Only“-Richtlinie, um einen besseren Überblick über die Datennutzung im Netzwerk zu erhalten.

- Bei Auswahl der Option **Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren** werden Benutzer über die Risiken informiert, die mit der Übertragung von Dokumenten einhergehen, die möglicherweise vertrauliche Daten enthalten. Diese Methode kann das Risiko von Datenverlusten ohne merkbare Abbremsung der Netzwerkgeschwindigkeit verringern.
- Stellen Sie in den Inhaltsregeln über die Mengen-Einstellung das Aufkommen an vertraulichen Daten ein, die vor dem Auslösen einer Regel gefunden werden sollen. Zum Beispiel löst eine Regel, die in einem Dokument nach einer Postanschrift sucht, mehr Data Control-Ereignisse aus als eine Regel, die nach mindestens 50 Adressen sucht.

Hinweis: Sophos bietet für jede Content Control List voreingestellte Mengen.

- Nutzen Sie die Data Control-Ereignisanzeige zur schnellen Filterung von Ereignissen. Alle Data Control-Ereignisse und -Maßnahmen werden zentral in Enterprise Console protokolliert. Sie können die Ereignisanzeige per Klick auf **Ansicht > Data Control-Ereignisse** aufrufen.
- Mit dem Report Manager lassen sich Trendberichte zu Data Control-Ereignissen nach Regel, Computer oder Benutzer sortiert erstellen.
- Anhand der benutzerdefinierten Desktop Messaging-Optionen können Sie Benutzern zusätzliche Hilfestellung beim Auslösen einer Maßnahme geben. Zum Beispiel können Sie einen Link zur Datensicherheitsrichtlinie Ihres Unternehmens angeben.
- Der ausführliche Protokollmodus bietet weitere Informationen zur Genauigkeit der Data Control-Regeln. Deaktivieren Sie die ausführliche Protokollierung wieder, wenn die Regeln ausgewertet wurden.

Hinweis: Die ausführliche Protokollierung muss auf jedem Computer aktiviert werden. Alle generierten Daten werden im Data Control-Protokoll des Computers verzeichnet. Im ausführlichen Protokollierungsmodus werden alle Zeichenketten erfasst, die mit den in einer Regel festgelegten Angaben übereinstimmen. Die Zusatzinformationen in einem Protokoll können zum Auffinden von Sätzen oder Zeichenketten in einem Dokument verwendet werden, das ein Data Control-Ereignis ausgelöst hat.

8.3 Implementieren einer Data Control-Richtlinie

Standardmäßig ist Data Control deaktiviert und es sind keine Regeln zur Überwachung oder Einschränkung der Übertragung von Dateien auf Speichergeräte oder in Anwendungen festgelegt. Es empfiehlt sich folgender Umgang mit Data Control:

1. Machen Sie sich mit Data Control vertraut:

- **Speichergeräte:** Data Control fängt alle Dateien ab, die mit Windows Explorer auf ein überwachtes Speichergerät kopiert werden (einschließlich des Windows-Desktops). Dateien, die jedoch direkt in einer Anwendung (z.B. Microsoft Word) gespeichert oder über die Befehlszeile übertragen werden, werden nicht erfasst.

Über die beiden folgenden Optionen können Sie erzwingen, dass alle Übertragungen auf ein überwachtes Speichergerät mit Windows Explorer erfolgen: Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren oder Übertragung sperren und Ereignis protokollieren. Bei Auswahl beider Optionen blockiert Data Control Versuche, Dateien direkt in einer Anwendung zu speichern oder über die Befehlszeile zu übertragen. Der Benutzer wird in einer Desktop-Benachrichtigung aufgefordert, die Übertragung mit Windows Explorer durchzuführen.

Wenn eine Data Control-Richtlinie nur Regeln mit der Maßnahme Dateiübertragung zulassen und Ereignis protokollieren umfasst, greift Data Control nicht beim Speichern in einer Anwendung oder der Übertragung über die Befehlszeile. Benutzer können Speichergeräte somit uneingeschränkt nutzen. Data Control-Ereignisse werden jedoch weiterhin ausschließlich bei Übertragungen mit Windows Explorer protokolliert.

Hinweis: Diese Einschränkung gilt nicht für die Überwachung von Anwendungen.

- **Anwendungen:** Data Control greift, wenn Dateien und Dokumente in überwachte Anwendungen hochgeladen werden. Damit nur von Benutzern eingeleitete Dateiübertragungen überwacht werden, werden einige Systemdateiverzeichnisse von Data Control ausgeschlossen. Nähere Informationen zum Scan-Umfang in Anwendungen entnehmen Sie bitte dem Abschnitt [Data Control-Scans in Anwendungen](#) (Seite 20).

Hinweis: Wenn Sie E-Mail-Clients überwachen, scannt Data Control alle Dateianhänge, jedoch nicht den Inhalt von E-Mails. Zum Scannen von E-Mail-Inhalten können Sie Sophos Email Security und Data Protection verwenden.

2. Überlegen Sie sich, welche Daten einer Kontrolle bedürfen und entsprechende Regeln erfordern. Sophos bietet eine Reihe von Regelvorlagen, die Ihnen die Erstellung der Data Control-Richtlinie erleichtert.

Wichtig: Bedenken Sie beim Erstellen von Inhaltsregeln, dass das Scannen von Inhalten sehr rechen- und zeitaufwändig ist. Testen Sie die Inhaltsregel auf jeden Fall vor der Integration in ein umfangreiches Netzwerk.

Hinweis: Beim Erstellen der ersten Richtlinie empfiehlt sich die Beschränkung auf die Erkennung personenbezogener Daten in Dokumenten. Sophos bietet zu diesem Zweck entsprechende Vorlagen.

3. Aktivieren Sie Data Control und wählen Sie in den Regeln die Option **Dateiübertragung zulassen und Ereignis protokollieren**, um kontrollierte Daten zu erkennen, jedoch nicht zu blockieren.

Wichtig: Diese Maßnahme sollte zunächst für alle Regeln übernommen werden. So können Sie die Wirksamkeit der Regeln ohne Beeinträchtigung der Benutzerproduktivität testen.

4. Übertragen Sie die Data Control-Richtlinie zunächst nur auf einige Computer, damit die Analyse ausgelöster Data Control-Ereignisse überschaubar bleibt.
5. Nutzen Sie die Data Control-Ereignisanzeige, um einen Überblick über die Datennutzung zu erhalten und Schwachstellen in der Testkonfiguration auszumachen. Sie können die Ereignisanzeige per Klick auf **Ansicht > Data Control-Ereignisse** aufrufen.
6. Korrigieren Sie die Richtlinie ggf. nach dem Test und übertragen Sie sie auf eine größere Gruppe von Computern. Jetzt sollten Sie folgende Punkte in Erwägung ziehen:
 - Auswählen der Maßnahmen **Benutzerbestätigte Übertragungen zulassen und Ereignis protokollieren** oder **Übertragung sperren und Ereignis protokollieren** für bestimmte Regeln.
 - Legen Sie am besten für jede Gruppe eine eigene Richtlinie an. So können Sie beispielsweise der Personalabteilung das Übertragen von personenbezogenen Daten erlauben, für die Mitglieder der übrigen Gruppen jedoch unterbinden.

Weitere Informationen zum Einrichten der Data Control-Richtlinie finden Sie in der Hilfe zu Sophos Enterprise Console.

8.4 Data Control-Scans in Anwendungen

Aus der folgenden Tabelle geht hervor, welche Inhalte und Handlungen in unterstützten Anwendungen gescannt werden bzw. vom Scanvorgang ausgeschlossen sind.

Im Support-Artikel 63016 werden bekannte Probleme in Zusammenhang mit Data Control erörtert (<http://www.sophos.de/support/knowledgebase/article/63016.html>).

Applications	Maßnahmen von Data Control
Internet-Browser	<p>Gescannt werden:</p> <ul style="list-style-type: none"> ■ Hochgeladene Dateien ■ Webmail-Anhänge ■ In Microsoft SharePoint hochgeladene Dateien <p>Nicht gescannt werden:</p> <ul style="list-style-type: none"> ■ Inhalte von Webmail-Nachrichten ■ Blog-Einträge ■ Heruntergeladene Dateien <p>Hinweis: In bestimmten Fällen werden Dateien beim Herunterladen gescannt.</p>

Applications	Maßnahmen von Data Control
E-Mail-Clients	<p>Gescannt werden:</p> <ul style="list-style-type: none"> ■ E-Mail-Anhänge <p>Nicht gescannt werden:</p> <ul style="list-style-type: none"> ■ Inhalte von E-Mail-Nachrichten ■ Weitergeleitete Anhänge ■ Über die Funktion zum Versenden von E-Mails in Anwendungen (z.B. Windows Explorer und Microsoft Office) erstellte Anhänge ■ Über die Option „Datei in E-Mail versenden“ in Windows Explorer erstellte Anhänge ■ Anhänge, die von einer E-Mail in eine andere E-Mail kopiert werden ■ Gespeicherte Anhänge <p>Hinweis: In bestimmten Fällen werden Dateien beim Speichern gescannt.</p>
Instant Messaging (IM) Clients	<p>Gescannt werden:</p> <ul style="list-style-type: none"> ■ Dateiübertragungen <p>Hinweis: Unter Umständen werden Dateien zwei Mal gescannt: beim Hochladen im IM-Client und bei Annahme durch den Benutzer. Beide Scans erfolgen auf dem Computer des Absenders.</p> <p>Nicht gescannt werden:</p> <ul style="list-style-type: none"> ■ Inhalte von IM-Nachrichten ■ Gesendete Dateien

9 Einrichten der Manipulationsschutz-Richtlinien

9.1 Empfohlene Einstellungen

Mit der Manipulationsschutz-Richtlinie können Sie verhindern, dass nicht autorisierte Benutzer (lokale Administratoren ohne hinreichende Fachkenntnisse) Sophos Sicherheitssoftware umkonfigurieren, deinstallieren oder deaktivieren. Unter nicht autorisierten Benutzern sind hierbei Benutzer ohne Manipulationsschutzkennwort zu verstehen.

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.

9.2 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.

Weitere Informationen zum Einrichten der Manipulationsschutz-Richtlinie finden Sie in der Hilfe zu Sophos Enterprise Console.

10 Einrichten von NAC-Richtlinien

10.1 Wann bieten sich die NAC-Standardrichtlinien an?

NAC-Richtlinien legen die Bedingungen fest, mit denen Computer als Voraussetzung für den Netzwerkzugriff übereinstimmen müssen. Standardmäßig haben alle Computer Zugriff auf das Netzwerk. Zur Einschränkung der Netzwerkzugriffsrechte müssen die NAC-Richtlinien entsprechend angepasst werden.

Mit den vordefinierten Standardrichtlinien können Sie die Konformität mit Sicherheitsrichtlinien sowohl auf verwalteten als auch auf nicht verwalteten Computern durchsetzen. Mit NAC Manager können Sie den Richtlinienmodus, die zugewiesenen Profile und Network Access Templates der Standardrichtlinien ändern.

Die folgenden Standardrichtlinien sind vorhanden:

- **Default:** Diese Richtlinie wird Computern zugewiesen, auf denen Compliance Agent installiert ist, und denen bisher keine andere Richtlinie zugewiesen wurde. Standardmäßig befinden sich Richtlinien im Modus „Report Only“. Die Richtlinie kann den Computer nur im Modus „Remediate“ (Korrigieren) oder „Enforce“ (Durchsetzen) korrigieren.
- **Managed:** Diese Richtlinie ist für Computer vorgesehen, auf denen Compliance Agent installiert ist und die von Enterprise Console verwaltet werden. Standardmäßig befinden sich Richtlinien im Modus „Report Only“. Die Richtlinie kann den Computer nur im Modus „Remediate“ (Korrigieren) oder „Enforce“ (Durchsetzen) korrigieren.
- **Unmanaged:** Diese Richtlinie ist für unternehmensexterne Computer vorgesehen. Sie führt keine Korrekturmaßnahmen durch. Compliance Dissolvable Agent verwendet die Richtlinie „Unmanaged“.

Weitere Informationen zum Ändern der Standardrichtlinien finden Sie in der Hilfe zu Sophos NAC Manager.

10.2 Implementieren einer NAC-Richtlinie

Zu Beginn verfügen alle Computer über die Standardrichtlinie. Mit Sophos NAC Manager können Sie Richtlinieneinstellungen bei Bedarf ändern und mit Enterprise Console auf Computer übertragen. Folgende Empfehlungen können beim Einrichten der NAC-Richtlinie hilfreich sein:

1. Erstellen oder importieren Sie über Enterprise Console Gruppen und installieren Sie Sophos Compliance Agent mithilfe des Assistenten zum Schutz von Computern.
2. Überprüfen Sie in NAC Manager, ob die NAC-Richtlinien die gewünschten Einstellungen, Profile und Access Templates enthalten.
3. Weisen Sie allen Enterprise Console-Gruppen über Enterprise Console die verwaltete NAC-Richtlinie zu.

Die Agenten führen die Konformitätsprüfung zunächst im Richtlinienmodus „Report Only“ durch.

4. Ermitteln Sie anhand der Reports in NAC Manager den aktuellen Konformitätszustand der Endpoints.

Die Reports verschaffen Ihnen einen Überblick über die tatsächliche Konformität einzelner Endpoints mit der NAC-Richtlinie.

5. Die Managed NAC-Richtlinie kann im NAC Manager geändert werden. Ändern Sie den Richtlinienmodus von „Report Only“ in „Remediate“.
6. Ermitteln Sie anhand der Reports in NAC Manager den aktuellen Konformitätszustand der Endpoints.

Im Laufe der Zeit sollten Endpoints, die nicht oder nur teilweise konform sind, automatisch korrigiert werden, um den allgemeinen Konformitätszustand zu verbessern.

7. Die Managed NAC-Richtlinie kann im NAC Manager geändert werden. Ändern Sie den Richtlinienmodus von „Remediate“ in „Enforce“.
8. Ermitteln Sie anhand der Reports in NAC Manager den aktuellen Konformitätszustand der Endpoints.

Nicht-konforme Endpoints müssen korrigiert werden, damit den Benutzern nicht der Zugriff auf Netzwerkressourcen verweigert wird.

Die NAC-Konfiguration wird in der Hilfe zu Sophos NAC Manager beschrieben.

11 Scan-Empfehlungen

Die im Folgenden genannten Scan-Optionen werden in der Anti-Virus- und HIPS-Richtlinie geregelt, gelten jedoch zum Teil auch für die Application Control-Richtlinie (z.B. Erweiterungen und Ausschlüsse). Beim Einrichten der Scan-Optionen können folgende Tipps hilfreich sein:

- Verwenden Sie möglichst die Voreinstellungen.
- Konfigurieren Sie Scans möglichst mit Enterprise Console statt auf dem Computer.
- Berücksichtigen Sie die Rolle des Computers (z.B. Desktop oder Server).
- 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.
- 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 Systempeicher auf Threats zu scannen. Der Systempeicher wird vom Betriebssystem genutzt. Sie können den Systempeicher regelmäßig bei aktivierten On-Access-Scans im Hintergrund scannen lassen. Sie können den Systempeicher auch im Rahmen eines geplanten Scans scannen. Die Option **Systempeicher scannen** ist nur bei neuen Softwareinstallationen standardmäßig aktiviert. Bei Software-Upgrades muss diese Option aktiviert werden.

12 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 28).



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

13 Geplante Scans

Für geplante Scans gelten folgende Empfehlungen:

- Verwenden Sie möglichst die Voreinstellungen.
- Mit geplanten Scans können Sie Threats und das Aufkommen unerwünschter oder überwachter 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.

14 On-Demand-Scans

On-Demand-Scans empfehlen sich unter folgenden Umständen:

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

15 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.

16 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.

17 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.

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.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>

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.