SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

Anleitung zur Richtlinieneinrichtung

Produktversion: 5.5

Inhalt

1 Einleitung

Diese Anleitung dient als Leitfaden zur Einrichtung von Richtlinien für Sophos Enterprise Console und Sophos Endpoint Security and Control.

Hinweis
Bestimmte Funktionen sind nur bei entsprechender Lizenzierung verfügbar.

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 Schnellstart-Anleitung zu Sophos Enterprise Console bereits gelesen haben.

Sämtliche Dokumente zu Enterprise Console finden Sie unter http://www.sophos.com/de-de/support/documentation/enterprise-console.aspx.

2 Allgemeine Empfehlungen

Bei der Installation von Enterprise Console werden Standard-Richtlinien für Sie erstellt. Diese Richtlinien werden auf neu erstellte Gruppen übertragen. Die Standardrichtlinien können lediglich eine allgemeine Schutzfunktion erfüllen. Wenn Sie Funktionen wie Network Access Control (NAC), Patch, Application Control, Data Control, Device Control oder Manipulationsschutz 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 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 Abonnement „Recommended“ angegeben ist. Beim Einrichten von Update-Richtlinien können folgende Tipps hilfreich sein:

- In der Regel bietet sich die Version „Recommended“ 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. Nähere Informationen entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console unter *Aktualisieren von Computern > Konfigurieren der Update-Richtlinie*.
- 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 der Laptop auf den in der Update-Richtlinie festgelegten primären (und anschließend den sekundären) Standort zu.

  Standort-Roaming ist nur möglich, wenn roamende Notebooks und feste Endpoints von der gleichen Instanz von Enterprise Console verwaltet werden und das gleiche Software-Abonnement aufweisen. In Firewalls von anderen Anbietern müssen Update-Standort-Anfragen und -Antworten zugelassen werden. Standardmäßig wird Port 51235 verwendet. Der Port kann jedoch geändert werden.

  Nähere Informationen entnehmen Sie bitte der Hilfe zu *Sophos Enterprise Console* unter *Aktualisieren von Computern > Konfigurieren der Update-Richtinie > Konfigurieren der Update-Server-Standorte*. Häufig gestellte Fragen zu Standort-Roaming werden im Sophos Support-Artikel 112830 (http://www.sophos.com/de-de/support/knowledgebase/112830.aspx) beantwortet.
- 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).

Achtung
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.
- Es empfiehlt sich ferner, die Option **Dateisamples automatisch an Sophos senden** zu aktivieren, um den Sophos Live-Schutz, der standardmäßig aktiviert ist, bestmöglich nutzen zu können.
- Aktivieren Sie die Erkennung schädlichen Datenverkehrs, welche Kommunikationen zwischen Endpoints und „Command-and-Control“-Servern, die mit einem Botnet oder einem anderen Malware-Angriff in Zusammenhang stehen, erkennt. Die Option **Erkennung schädlichen Datenverkehrs** ist auf neuen Installationen von Enterprise Console 5.3 oder höher standardmäßig aktiviert. Wenn Sie ein Upgrade von einer älteren Version von Enterprise Consolevorgenommen haben, müssen Sie diese Option aktivieren, um die Funktion nutzen zu können.

  Hinweis
  Die Erkennung schädlichen Datenverkehrs wird momentan nur unter Windows 7 und neueren Nicht-Server-Betriebssystemen unterstützt. Sophos Live Protection ist erforderlich.

- 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.

Näheres hierzu entnehmen Sie bitte dem Sophos Support-Artikel 114345 (http://www.sophos.com/de-de/support/knowledgebase/114345.aspx).

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. 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. Sophos Live Protection ist für die Funktionen „Erkennung schädlichen Datenverkehrs“ und „Download-Reputation“ erforderlich.

- Stellen Sie sicher, dass die Optionen **Live Protection für On-Access-Überprüfung** und **Live Protection für On-Demand-Überprüfung** ausgewählt sind. Wenn eine Datei von einem Antiviren-Scan auf einem Endpoint als verdächtig eingestuft wurde, anhand der Threatkennungsdateien (IDEs) auf dem Computer jedoch nicht festgestellt 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 SophosLabs 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.
- Wählen Sie die Option **Dateisamples automatisch an Sophos senden** aus. 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 Live Protection und die Option **Dateisamples automatisch an Sophos senden** aktiviert sind 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.com/de-de/support/knowledgebase/62637.aspx). 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.

3. 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 31) und Geplante Scans (Seite 32).
   b) Wählen Sie Bereinigungsoptionen für Viren/Spyware.
4. Aktivieren Sie die Erkennung verdächtiger Dateien.
   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** in den Scan-Einstellungen.
   c) Wählen Sie Bereinigungsoptionen für verdächtige Dateien.
   d) Lassen Sie ggf. alle erlaubten Programme zu.
5. Aktivieren Sie die Erkennung von schädlichem und verdächtigem Verhalten, Pufferüberläufen und schädlichem Datenverkehr (Verhaltensüberwachung).
   Anhand der Optionen werden laufende Prozesse beständig auf schädliches oder verdächtiges Verhalten überwacht. Die Methoden eignen sich zum Abwehren von Sicherheitsrisiken.
   a) Stellen Sie sicher, dass die Verhaltensüberwachung für On-Access-Scans aktiviert ist. Die Option ist standardmäßig aktiviert.
   b) Stellen Sie sicher, dass die Option **Erkennung schädlichen Datenverkehrs** ausgewählt ist.
   c) Wählen Sie die Option **Nur benachrichtigen**, um nur verdächtiges Verhalten und Pufferüberläufe zu erkennen. Diese Option ist standardmäßig aktiviert.
   d) Lassen Sie Programme und Dateien zu, die Sie weiterhin verwenden möchten.

e) 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. Näheres hierzu entnehmen Sie bitte dem Sophos Support-Artikel 50160 (http://www.sophos.com/de-de/support/knowledgebase/50160.aspx).

6. 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.

   Näheres hierzu entnehmen Sie bitte dem Sophos Support-Artikel 13815 (http://www.sophos.com/de-de/support/knowledgebase/13815.aspx).

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

   Über die Option werden Websites blockiert, die bekanntermaßen Malware hosten. Zudem werden Downloads auf schädliche Inhalte gescannt.

   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 **Content-Scanning Ein** oder **Wie On-Access** aus, um heruntergeladene schädliche 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.

   d) Stellen Sie sicher, dass die Reputationsprüfung von Dateien aktiviert ist.

Hinweis
Außerdem können Sie mit der Web Control-Richtlinie kontrollieren, welche Seiten Benutzer aufrufen können, indem Sie URLs in 14 Kategorien unangemessener Websites filtern. Nähere Informationen zum Einrichten einer Web Control-Richtlinie finden Sie unter Empfohlene Einstellungen (Seite 26).

Nähere Informationen zum Einrichten der Antivirus- und HIPS-Richtlinien entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console.

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 System- und Softwarevoraussetzungen finden Sie auf der Sophos Website: (http://www.sophos.com/de-de/products/all-system-requirements).

Achtung
Firewall-Richtlinien müssen vor der Nutzung konfiguriert werden. Die Zuweisung einer nicht geänderten Standardrichtlinie mit Sophos Enterprise Console 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 Standardrichtlinie, 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. Die Richtlinien decken unterschiedliche Anwendungen ab und sind unterschiedlich restriktiv. Für mehrere Gruppen in Enterprise Console müssen mehrere Richtlinien erstellt werden.

- Es wird davon abgeraten, nur eine Sophos Client Firewall-Richtlinie zu verwenden. 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.

Netwerkübergreifende 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 wird 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 **Ereignisse** > **Firewall-Ereignisse** aufrufen.

- Überprüfen Sie die erstellten Regeln in der Ereignisanzeige. Unter Umständen werden mehrere Firewall-Ereignisse zu unterschiedlichen Maßnahmen einer Anwendung angezeigt. Eine Anwendungsregel muss jedoch alle Maßnahmen zu einer bestimmten Anwendung abdecken. Für ein E-Mail-Programm können etwa jeweils ein Ereignis beim Senden und beim Empfangen einer E-Mail angezeigt werden. Eine Anwendungregel muss beide Maßnahmen 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 auf der Registerkarte **Allgemein** im Bereich **Angewandter Standort** der erweiterten Firewall-Richtlinie die zu übertragende Firewall-Konfiguration. 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.

Achtung
Bei lokalen Subnetzregeln in sekundären Konfigurationen ist Vorsicht geboten. Laptops, die außerhalb des Unternehmens eingesetzt werden, stellen unter Umständen eine Verbindung zu einem unbekannten 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 der 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.

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

1. Installieren Sie Sophos Client Firewall auf einer Gruppe von Testcomputern, 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 Console im Fenster **Richtlinien** auf **Firewall** und wählen Sie die Option **Richtlinie erstellen** aus. Geben Sie der Richtlinie einen Namen und doppelklicken Sie darauf.
   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**.
      - Klicken Sie im Assistenten 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 **Ereignisse** > **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 Hilfe zu Sophos Enterprise Console unter *Konfigurieren von Richtlinien* > *Firewall-Richtlinie*.

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 unterschiedlichen Maßnahmen einer Anwendung angezeigt. Eine Anwendungsregel muss jedoch alle Maßnahmen zu einer bestimmten Anwendung abdecken. Für ein E-Mail-Programm können etwa jeweils ein Ereignis beim Senden und beim Empfangen einer E-Mail angezeigt werden. Eine Anwendungregel muss beide Maßnahmen 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.).
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 entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console unter *Konfigurieren von Richtlinien* > *Firewall-Richtlinie*.

Hinweis
Als Alternative zur Überwachung des Datenverkehrs und der Erstellung von Regeln in der Firewall-Ereignisanzeige können Sie bei kleinen Netzwerken oder Einzelplatzrechnern mit Windows 7 oder älter Sophos Client Firewall auf einem Testcomputer installieren und im **interaktiven Modus** konfigurieren. 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. Weitere Informationen finden Sie in der Sophos Endpoint Security and ControlHilfe.

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 Ereignisansicht zu Application Control lässt sich die Nutzung von Anwendungen in Ihrem Unternehmen prüfen. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **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 **Ereignisse** > **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. Nähere Informationen zum Einrichten der Application Control-Richtlinie entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console.

Hinweis
Application Control kann zum Blockieren des von der Patch-Funktion verwendeten Skripts „CScript.exe“ konfiguriert werden. Wenn Sie Application Control und Patch nutzen, stellen Sie sicher, dass **Microsoft WSH CScript** nicht in der Kategorie **Programmierungs-/Skripting-Tool** blockiert wird. Standardmäßig werden Programmierungs-/Skripting-Tools zugelassen.

7 Einrichten von Data Control-Richtlinien

7.1 Definieren einer 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.

7.2 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 merkliche 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 **Ereignisse** > **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.

7.3 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 18).

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 erleichtern.

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 **Ereignisse** > **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 die Übertragung personenbezogener Daten erlauben, für die Mitglieder der übrigen Gruppen jedoch unterbinden.

Nähere Informationen zum Einrichten der Data Control-Richtlinie entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console.

7.4 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.

Die komplette Liste bekannter Beschränkungen in Zusammenhang mit Data Control finden Sie im Sophos Support-Artikel 63016 (http://www.sophos.com/de-de/support/knowledgebase/63016.aspx).

Anwendungen	Maßnahmen von Data Control
Internet-Browser	**Gescannt werden:** • Hochgeladene Dateien • Webmail-Anhänge • In Microsoft SharePoint hochgeladene Dateien **Nicht gescannt werden:** • Inhalte von Webmail-Nachrichten • Blog-Einträge • Heruntergeladene Dateien **Hinweis** In bestimmten Fällen werden Dateien beim Herunterladen gescannt.

Anwendungen	Maßnahmen von Data Control
E-Mail-Clients	**Gescannt werden:** • E-Mail-Anhänge **Nicht gescannt werden:** • 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 **Hinweis** In bestimmten Fällen werden Dateien beim Speichern gescannt.
Instant Messaging (IM) Clients	**Gescannt werden:** • Dateiübertragungen **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. **Nicht gescannt werden:** • Inhalte von IM-Nachrichten • Gesendete Dateien

8 Einrichten von Device Control-Richtlinien

8.1 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 **Ereignisse** > **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. Die komplette Liste der unterstützten sicheren Wechselmedien ist dem Sophos Support-Artikel 63102 zu entnehmen (http://www.sophos.com/de-de/support/knowledgebase/63102.aspx).
- 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.

Achtung
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.

8.2 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 **Ereignisse** > **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.
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 Hilfe zu Sophos Enterprise Console.

9 Einrichten von Manipulationsschutz-Richtlinien

9.1 Informationen zur Manipulationsschutz-Richtlinie

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. Für weitere Informationen, siehe Empfohlene Einstellungen (Seite 5).

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 (wie Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate oder Sophos Remote Management System) 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 **Ereignisse** > **Manipulationsschutz-Ereignisse** aufrufen.

9.2 Erweiterter Manipulationsschutz

Der erweiterte Manipulationsschutz baut auf dem Manipulationsschutz auf. Wenn der erweiterte Manipulationsschutz aktiviert ist, werden die folgenden Aktionen für Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System und Sophos Endpoint Defense blockiert:

- Stoppen der Dienste über die Services-UI
- Beenden der Dienste über die Task-Manager-UI
- Ändern der Dienstkonfiguration über die Services-UI
- Stoppen der Dienste/Bearbeiten der Dienstkonfiguration über die Befehlszeile

- Wird deinstalliert
- Wird erneut installiert
- Beenden von Prozessen über die Task-Manager-UI (erwünscht)
- Geschützte Dateien oder Ordner löschen oder ändern
- Systemgeschützte Registrierungsschlüssel löschen oder ändern

Wichtig
Zum Aktivieren des erweiterten Manipulationsschutzes muss der Manipulationsschutz aktiviert sein.

9.3 Implementieren der Manipulationsschutz-Richtlinie

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

Hinweis
Wenn Sie bei der Installation den erweiterten Manipulationsschutz aktiviert haben, ist der Manipulationsschutz bereits aktiviert.

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.

   Wichtig
   Wenn der Manipulationsschutz deaktiviert ist, wird der erweiterte Manipulationsschutz automatisch ebenfalls deaktiviert.

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

10 Einrichten der Patch-Richtlinien

10.1 Informationen zur Patch-Richtlinie

Mit Patch-Richtlinien wird festgestellt, ob die aktuellen Sicherheits-Patches auf den Computern installiert wurden.

Anhand der von den SophosLabs bereitgestellten Bewertung können Sie ermitteln, welche Sicherheits-Patch-Probleme das höchste Risiko bergen, und diese umgehend beheben. Die Bewertungen der SophosLabs basieren auf den aktuellen Exploits und weichen daher unter Umständen vom vom Hersteller angegebenen Schweregrad ab.

Beim Einrichten Ihrer Patch-Richtlinie können Sie mit der Ereignisanzeige der Patch-Analyse feststellen, ob Patches auf den Computern im Unternehmen fehlen. Hier finden Sie Informationen zu Sicherheits-Patches und können die Ergebnisse der Patch-Analyse abrufen. Nach der Aktivierung der Patch-Analyse in der Richtlinie können Sie den Patch-Status nach Computer, Gruppe oder Threat anzeigen. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **Patch-Analyse-Ereignisse** aufrufen.

Hinweis
Patch verwendet „CScript.exe“, das mit Application Control blockiert werden kann. Wenn Sie Application Control und Patch nutzen, stellen Sie sicher, dass **Microsoft WSH CScript** nicht in der Kategorie **Programmierungs-/Skripting-Tool** der **Application Control**-Richtlinie blockiert wird. Standardmäßig werden Programmierungs-/Skripting-Tools von Application Control zugelassen.

10.2 Implementieren der Patch-Richtlinie

Zu Beginn verfügen alle Computer über die Standardrichtlinie. Die Patch-Analyse ist in der Standardrichtlinie deaktiviert.

Nach der Aktivierung der Patch-Analyse leiten die Computer die Analyse ein. Dies kann einige Minuten dauern. Weitere Prüfungen erfolgen in den in der Richtlinie festgelegten Zeitabständen (das Standard-Intervall lautet „täglich“).

Hinweis
Wenn die Computer die Analyse durchführen, bevor Enterprise Console zum ersten Mal Patch-Daten von Sophos heruntergeladen hat, werden keine Ereignisse in der Patch-Ereignisanzeige angezeigt. Der Download kann mehrere Stunden in Anspruch nehmen. Im Feld **Patch-Updates** der **Patch-Analyse – Ereignisanzeige** können Sie überprüfen, ob der Vorgang abgeschlossen wurde.

Folgende Empfehlungen können beim Einrichten der Patch-Richtlinie hilfreich sein:

1. Installieren Sie den Patch Agent mit Hilfe des Assistenten zum Schutz von Computern. Wählen Sie auf der Seite zur **Funktionsauswahl** die Option **Patch** aus.

Hinweis
Sie müssen die Computer erneut mit dem Assistenten zum Schutz von Computern schützen, wenn Enterprise Console bereits ausgeführt wird, der Patch Agent jedoch nicht installiert ist.

2. Aktivieren Sie die Patch-Analyse in der Standard-Patch-Richtlinie.

   Zunächst ist eine Patch-Richtlinie vorhanden.
3. Mit der Ereignisanzeige der Patch-Analyse können Sie sich Computer mit fehlenden Patches sowie Computer, die sich nicht auf dem neuesten Stand befinden, anzeigen lassen. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **Patch-Analyse-Ereignisse** aufrufen.

   Hinweis
   Fehlende Patches müssen manuell auf Computern installiert werden.

4. Wenn Sie die Patch-Richtlinie aktivieren bzw. deaktivieren oder unterschiedlichen Gruppen unterschiedliche Patch-Analyse-Intervalle zuweisen möchten, erstellen Sie unterschiedliche Richtlinien für die jeweiligen Gruppen.

Nähere Informationen zum Einrichten der Patch-Richtlinie entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console.

11 Einrichten von Web Control-Richtlinien

11.1 Empfohlene Einstellungen

Bei der Konfiguration von Web Control stehen zwei Richtlinien zur Auswahl: Kontrolle unangebrachter Websites und Vollständige Web Control. Je nach der ausgewählten Richtlinie gelten unterschiedliche Empfehlungen. Beim Einrichten von Web Control-Richtlinien können folgende Tipps hilfreich sein:

Kontrolle unangebrachter Websites

- Sehen Sie sich die den jeweiligen Website-Kategorien zugewiesenen Maßnahmen an und passen Sie sie an die Anforderungen im Unternehmen an. Wenn Sie den unterschiedlichen Computergruppen jeweils unterschiedliche Web-Zugriffsrechte zuweisen möchten, erstellen Sie gruppenspezifische Richtlinien. Es kann sich beispielsweise anbieten, den Zugriff auf bestimmte Websites (wie etwa Facebook) nur der Personalabteilung zu gewähren.
- Legen Sie bereits vor der Einführung einer Richtlinie eine Liste mit Website-Ausschlüssen fest. Mit Hilfe der Registerkarte **Website-Ausschlüsse** können Sie manuell Websites angeben, die Sie von der Richtlinie ausschließen möchten. Dies bietet sich etwa an, wenn Sie eine Reihe lokaler Web-Adressen nicht filtern möchten oder Websites in einer Kategorie blockieren möchten, die normalerweise zulässig sind.
- Mit Hilfe der Web Control – Ereignisanzeige können Sie gefilterte Web-Ergebnisse schnell filtern. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **Web-Ereignisse** aufrufen. Je nach angezeigter Maßnahme können Sie die Einstellungen der Website-Kategorien anpassen.

Vollständige Web Control

Wichtig
Zur Nutzung der Richtlinie der Vollständigen Web Control ist eine Sophos Web Appliance oder Security Management Appliance erforderlich.

- Die Konfigurationsanleitungen zur Sophos Web Appliance und zur Security Management Appliance enthalten allgemeine Anweisungen zur Einrichtung der Appliance. Der Setup-Assistent der Appliance unterstützt Sie bei der Auswahl der Einstellungen für Ihr Unternehmen.
- Unter Umständen bietet sich an, unterschiedlichen Benutzergruppen unterschiedliche Richtlinien zuzuweisen. Der Online-Dokumentation zur Web Appliance können Sie weitere Informationen entnehmen.

  Die Dokumentation zur Sophos Web Appliance steht unter http://wsa.sophos.com/docs/wsa/ bereit.
- Vor dem Implementieren einer Richtlinie sollten Sie Ausschlüsse für die Web Control-Richtlinie festlegen. Mit der „Special Hours“-Option können Sie beispielsweise allen oder einigen Benutzern Zugriff auf bestimmte Seiten außerhalb der festen Arbeitszeiten (z.B. in der Mittagspause) gewähren. Sie können ferner weitere Richtlinien („Additional Policies“) erstellen, die sich nur auf bestimmte Benutzer beschränken und Ausnahmen zur Standardrichtlinie und zeitlich beschränkten Richtlinie darstellen.

- Legen Sie fest, welche Maßnahme die Web Appliance ggf. ergreifen soll, wenn eine Website in keine Kategorie eingeordnet werden kann. Die Option **Browsen verweigern, wenn die Website-Kategorie nicht bestimmt werden kann.** ist standardmäßig ***nicht*** aktiviert. Wenn die Kategorisierung also nicht möglich ist, können Benutzer ungehindert browsen. Wenn die Option aktiviert ist, werden nicht kategorisierbare URLs so lange gesperrt, bis der Dienst wieder funktioniert.

Nähere Informationen entnehmen Sie bitte der Dokumentation zu Sophos Enterprise Console und zur Sophos Web Appliance.

11.2 Implementieren einer Web Control-Richtlinie

Zunächst müssen Sie festlegen, welchen Webfilterungs-Modus Sie verwenden möchten: Kontrolle unangebrachter Websites oder Vollständige Web Control. Zur Nutzung der Richtlinie der Vollständigen Web Control ist eine Sophos Web Appliance oder Security Management Appliance erforderlich.

Nähere Informationen zum Einrichten der Web Control-Richtlinie entnehmen Sie bitte der Sophos Enterprise ConsoleHilfe.

11.2.1 Implementieren einer Richtlinie zur Kontrolle unangebrachter Websites

Die Basisoption von Web Control umfasst 14 Website-Kategorien. Sie schützt Benutzer vor dem Aufrufen unangebrachter Websites. Beim Einrichten von Web Control-Richtlinien können folgende Tipps hilfreich sein: Detaillierte Anweisungen entnehmen Sie bitte der Dokumentation zu Enterprise Console.

1. Stellen Sie sicher, dass die Web Control-Richtlinie aktiviert ist.
2. Wenn Sie Internetnutzungsrichtlinien im Unternehmen implementiert haben, empfiehlt sich, die Einstellungen daran auszurichten, und so zu unterbinden, dass Benutzer potenziell unangebrachte Websites aufrufen.
3. Wenn Sie den unterschiedlichen Computergruppen jeweils unterschiedliche Zugriffsrechte auf Websites zuweisen möchten, erstellen Sie gruppenspezifische Richtlinien.
4. Überlegen Sie sich, welche Computergruppen von Web Control erfasst werden sollen und welcher Richtlinientyp sich für die jeweiligen Computergruppen anbietet.
5. Sehen Sie sich die Standardmaßnahmen für die jeweiligen Website-Kategorien an. Wenn Sie eine andere Maßnahme zuweisen möchten, wählen Sie sie aus dem Dropdown-Menü aus. Überlegen Sie sich, welche Kategorien blockiert bzw. zugelassen werden sollen und beim Aufrufen welcher Kategorien eine Warnung angezeigt werden soll.
6. Wählen Sie die Websites aus, die Sie von der der Filterung ausschließen möchten, und nehmen Sie sie in die Liste **zulässiger** oder **blockierter Websites** auf.

> **Hinweis**
> Bei Überschneidungen bzw. Konflikten zwischen den Maßnahmen „Blockieren“ und „Zulassen“ hat die Maßnahme „Blockieren“ Vorrang. Wenn die gleiche IP-Adresse etwa in der Liste „Blockieren“ und „Zulassen“ enthalten ist, wird die Website blockiert. Wenn ferner eine Domäne in der Liste „Blockieren“, eine ihrer Unterdomänen jedoch in der Liste „Zulassen“ enthalten ist, werden die Domäne und sämtliche Unterdomänen blockiert.

7. Mit der Web Control-Ereignisanzeige können Sie die Filterergebnisse aufrufen. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **Web-Ereignisse** aufrufen. Mit der Ereignisanzeige können Sie Web-Ereignisse abrufen. Je nach den Ergebnissen können Sie Änderungen an den Einstellungen vornehmen.

Nähere Informationen entnehmen Sie bitte der Dokumentation zu Enterprise Console.

11.2.2 Implementieren einer Richtlinie zur Vollständigen Web Control

In diesem Modus wird eine umfangreiche Web-Richtlinie verwendet. Die umfassende Web-Richtlinie wird durchgesetzt. Zudem werden umfassende Reports zum Datenverkehr im Web erstellt. Für diese Option ist eine Sophos Web Appliance oder eine Security Management Appliance erforderlich.

1. Konfigurieren Sie die Sophos Web Appliance oder die Security Management Appliance anhand der Anweisungen der Dokumentation zur Appliance und stellen Sie sicher, dass **Endpoint Web Control** aktiviert ist.
2. Stellen Sie sicher, dass Web Control in Enterprise Console aktiviert ist.
3. Wenn Sie Internetnutzungsrichtlinien im Unternehmen implementiert haben, empfiehlt sich, die Einstellungen daran auszurichten, und so zu unterbinden, dass Benutzer potenziell unangebrachte Websites aufrufen.
4. Wenn Sie den unterschiedlichen Benutzergruppen jeweils unterschiedliche Zugriffsrechte auf Websites zuweisen möchten, erstellen Sie benutzerspezifische Richtlinien.
5. Überlegen Sie genau, welche Websites gesteuert werden sollen. Welche Kategorien sollen für Benutzer nicht zugänglich sein? Welche Kategorien sollen zugänglich sein? Zu welchen Kategorien soll eine Warnung angezeigt werden?
6. Überlegen Sie sich, welche Websites ausgeschlossen werden sollen, und fügen Sie sie zur „Local Site List“ der Appliance hinzu.
7. Mit der Vollständigen Web Control können Sie Sophos LiveConnect verwenden. Sie können die Appliance zur Verwendung von LiveConnect konfigurieren. So werden Richtlinien-Updates auf die Benutzer übertragen. Report-Daten von den Computern werden auch dann hochgeladen, wenn keine Verbindung zum Netzwerk besteht.

Nähere Informationen entnehmen Sie bitte der Dokumentation zu Sophos Enterprise Console und zur Sophos Web Appliance.

12 Einrichten von Exploit-Abwehr-Richtlinien

12.1 Empfohlene Einstellungen

In der Exploit-Abwehr-Richtlinie wird festgelegt, wie die Sicherheitssoftware vor Ransomware und anderen Formen von Malware-Angriffen schützt.

Hinweis
Alle Optionen für die Exploit-Abwehr sind standardmäßig aktiviert.

Wir empfehlen, die Standardeinstellungen zu verwenden.

12.2 Implementieren einer Exploit-Abwehr-Richtlinie

Anwendungen mit Sicherheitslücken sind standardmäßig geschützt. Gehen Sie mit Bedacht vor, wenn Sie Anwendungen von der Exploit-Abwehr ausschließen. Diese sind weiterhin durch CryptoGuard und Sicheres Surfen geschützt.

Verfahren Sie zum Implementieren einer Exploit-Abwehr-Richtlinie wie folgt:

1. Alle Optionen für die Exploit-Abwehr sind standardmäßig aktiviert. Wir empfehlen, die Standardeinstellungen zu verwenden. Sie sollten etwaige Exploit-Abwehr-Ereignisse für einen gewissen Zeitraum beobachten, bevor Sie die Einstellungen ändern.
2. Verwenden Sie zur Beobachtung von Exploit-Abwehr-Ereignissen die Exploit-Abwehr-Ereignisanzeige. Sie können die Ereignisanzeige per Klick auf **Ereignisse** > **Exploit-Abwehr-Ereignisse** aufrufen.
3. Ändern Sie die Exploit-Abwehr-Richtlinie entsprechend den Ergebnissen Ihrer Überwachung. Sie können z. B. bestimmte Anwendungen oder Exploit-Ereignisse von der Exploit-Abwehr ausschließen. Nähere Informationen finden Sie in der Hilfe zu Sophos Enterprise Console unter *Konfigurieren von Richtlinien* > *Exploit-Prevention-Richtlinie*.

   Wichtig
   Für optimale Sicherheit empfehlen wir, den Ausschluss basierend auf dem Thumbprint des Exploits vorzunehmen anstatt die ganze Anwendung auszuschließen.

   a) Erstellen Sie eine neue Richtlinie oder ändern Sie die Standardrichtlinie.

   b) Prüfen Sie die Richtlinie auf Schwachstellen.

   c) Bei unterschiedlichen Anforderungen unterteilen Sie die Gruppe und erstellen Sie zusätzliche Richtlinien.
4. Weisen Sie die Richtlinie entsprechend den Erfordernissen zu.

Nähere Informationen zum Einrichten von Exploit-Abwehr-Richtlinien entnehmen Sie bitte der Hilfe zu Sophos Enterprise Console.

13 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 Console 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.

14 On-Access-Scans

Für On-Access-Scans gelten folgende Empfehlungen:

- Verwenden Sie möglichst die Voreinstellungen.
- On-Access-Scans beim **Lesen**, **Schreiben** und **Umbenennen** sind standardmäßig nur bei neuen Softwareinstallationen aktiviert. Bei Software-Upgrades müssen diese Optionen aktiviert werden.
- 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 zur Verwendung der Antivirus- und HIPS-Richtlinie in Kombination mit Verschlüsselungssoftware entnehmen Sie bitte dem Sophos Support-Artikel 12790 (http://www.sophos.com/de-de/support/knowledgebase/12790.aspx).
- Wenn Sie On-Access-Scans nicht benötigen, sollten zumindest geplante Scans eingerichtet werden. Für weitere Informationen, siehe Geplante Scans (Seite 32).

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

15 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.
- 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.

16 On-Demand-Scans

On-Demand-Scans empfehlen sich unter folgenden Umständen:

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

17 Auschluss von Objekten von der Überprüfung

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.

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

18 Technischer Support

Sie können sich wie folgt an den technischen Support von Sophos wenden:

- Rufen Sie das Sophos Community-Forum unter http://community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Begleitmaterial zu den Produkten finden Sie hier: www.sophos.com/de-de/support/documentation.aspx
- Öffnen Sie ein Service Ticket unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

19 Rechtliche Hinweise