

# SOPHOS

## Sophos Endpoint Security and Control Windows XPe/Windows Embedded Standard Test-Anleitung

Produktversion: 9.0  
Stand: September 2009



# Inhalt

- 1 Einleitung.....3
- 2 Test-Vorbereitung.....3
- 3 Installation von Sicherheitssoftware.....3
- 4 Testen der Threat-Erkennung.....4
- 5 Testen von Application Control.....5
- 6 Testen von Data Control.....5
- 7 Testen von Device Control.....6
- 8 Copyright.....7

# 1 Einleitung

Diese Anleitung richtet sich an Netzwerkadministratoren, die Computer unter Windows XP Embedded (Windows XPe) oder Windows Embedded Standard schützen möchten.

Die Embedded-Versionen von Windows werden häufig an die Bedürfnisse der Benutzer angepasst und unterscheiden sich daher mitunter sehr. Die vorliegende Anleitung kann aus diesem Grund nicht auf alle Einzelheiten eingehen. Vielmehr wird hier erläutert, wie sich nach der Installation feststellen lässt, ob Sophos Sicherheitssoftware ordnungsgemäß läuft.

Es wird davon ausgegangen, dass Sie bereits zu einem früheren Zeitpunkt mit **Sophos Enterprise Console** Sophos Software in Ihrem Netzwerk installiert und verwaltet haben.

Die Anleitung deckt folgende Themen ab:

- Installation von Sophos Sicherheitssoftware auf Computern mit Windows XPe/Windows Embedded Standard.
- Testen der Software-Update-Funktion
- Testen der Threat-Erkennung
- Testen von Application Control, Data Control und Device Control.

**Wichtig:** Wenn Sie alle in der Anleitung beschriebenen Tests durchführen, ist Sophos bestrebt, in Einklang mit der gängigen Praxis Support zu leisten. Nähere Informationen finden Sie im Support-Artikel **63797** (<http://www.sophos.de/support/knowledgebase/article/63797.html>).

## 2 Test-Vorbereitung

Vorbereitung:

- Wählen Sie Endpoints mit Windows XPe/Windows Standard Embedded für die Tests aus.
- Stellen Sie sicher, dass Sie die EICAR-Virenerkennungstestdatei auf den Testcomputern installiert haben bzw. installieren können.
- Sie müssen **MSN Messenger Live** für den Test von Application Control installieren.

## 3 Installation von Sicherheitssoftware

Führen Sie vor dem Test folgende Schritte durch:

- Installieren Sie die Sicherheitssoftware auf Endpoints.
- Stellen Sie sicher, dass die Software Updates bezieht.

### 3.1 Software-Installation

Die Installation von Sophos Endpoint Security and Control 9.0 erfolgt wie bei allen Windows-Endpoints.

Führen Sie einen der folgenden Schritte durch:

- **Automatische Installation.** Suchen Sie die Testcomputer in Enterprise Console und stellen Sie sicher, dass Sie über eine gültige Update-Richtlinie verfügen. Wählen Sie die gewünschten Computer aus, rechtsklicken Sie auf die Auswahl und klicken Sie auf **Computer schützen**.
- **Manuelle Installation.** Navigieren Sie auf den Test-Computern zu dem Ordner, von dem die Endpoints Updates beziehen und führen Sie das Sophos Installationsprogramm aus.

Hinweis: Sie finden den Ordner, von dem die Computer Updates beziehen unter **Bootstrap-Verzeichnisse** in Enterprise Console.

## 3.2 Überprüfen der Update-Funktion

Sie sollten prüfen, ob die Test-Computer Sophos-Updates beziehen.

Führen Sie auf den Test-Computern folgende Schritte durch:

1. Rechtsklicken Sie in der Taskleiste auf **Jetzt updaten**. Warten Sie, bis das Update abgeschlossen ist.
2. Öffnen Sie Sophos Endpoint Security and Control.
3. Überprüfen Sie auf der Startseite im **Statusfeld**, ob sich der Zeitstempel im Bereich **Letztes Update** geändert hat.

# 4 Testen der Threat-Erkennung

## 4.1 Überprüfen der Funktionalität der Threat-Erkennung

Mit Hilfe eines EICAR-Tests lässt sich ermitteln, ob Sophos Endpoint Security and Control Threats erkennt. Verfahren Sie hierzu wie folgt:

1. Versuchen Sie, eine EICAR-Testdatei auf den Testcomputer zu kopieren (bzw. auszuführen, wenn sich die EICAR-Datei bereits auf dem Computer befindet).

Auf den Testcomputern sollte ein Viren-Alert angezeigt werden.

2. Überprüfen Sie, ob sich die EICAR-Datei im Quarantäne-Manager befindet und alle Details korrekt sind.

## 4.2 Überprüfen von Alerts

Wechseln Sie zu **Enterprise Console** und verfahren Sie wie folgt:

1. Überprüfen Sie, ob auf den Registerkarten der Computerlistenansicht Folgendes angezeigt wird: Virennamen, Auftrittsort und Erkennungszeitpunkt.
2. Überprüfen Sie die angezeigten Details der Testcomputer auf ihre Richtigkeit.

Jetzt müssen Sie die Alerts löschen.

## 4.3 Löschen von Alerts

1. Löschen Sie auf den Testcomputern den Alert vom Quarantäne-Manager.
2. Löschen Sie in Enterprise Console den Alert im Dialogfeld **Alerts und Fehler löschen**.

# 5 Testen von Application Control

## 5.1 Konfigurieren von Application Control

1. Öffnen Sie in Enterprise Console eine Application Control-Richtlinie.
2. Konfigurieren Sie die Richtlinie so, dass MSN Live Messenger gesperrt wird.
3. Übertragen Sie die Richtlinie auf die Testcomputer.
4. Überprüfen Sie in Enterprise Console, ob die Richtlinienänderung übernommen wurde und ob die Testcomputer mit der Richtlinie konform sind.

## 5.2 Überprüfen der Funktionalität von Application Control

1. Rechtsklicken Sie auf den Testcomputern auf das SESC-Symbol und wählen Sie die Option **Jetzt updaten**.
2. Versuchen Sie, MSN Live Messenger zu installieren und zu öffnen.
3. Überprüfen Sie, ob ein Alert angezeigt wird. Überprüfen Sie, ob die Anwendung im Quarantäne-Manager angezeigt wird und alle Details (einschließlich Typ) korrekt sind.
4. Prüfen Sie in Enterprise Console die Computerlistenansicht und die Seite mit den Computerdetails.

## 5.3 Löschen von Alerts und Zurücksetzen der Richtlinie

1. Löschen Sie auf den Testcomputern die Alerts vom Quarantäne-Manager.
2. Setzen Sie die Application Control-Richtlinie in Enterprise Console wieder auf die ursprünglichen Einstellungen zurück.
3. Überprüfen Sie, ob Endpoint und Konsole mit der geänderten Richtlinie konform sind.

# 6 Testen von Data Control

## 6.1 Konfigurieren von Data Control

1. Erstellen Sie in Enterprise Console eine Data Control-Richtlinie und öffnen Sie sie.
2. Klicken Sie im Fenster **Richtlinienregeln** auf **Regeln verwalten**.

3. Klicken Sie im Dialogfeld **Verwaltung der Data Control-Regeln** auf die Option **Inhaltsregel hinzufügen**.
4. Geben Sie der Regel einen Namen. Klicken Sie unter **Regelinhalt** auf den Link im Bereich **Datei enthält**.
5. Wählen Sie im Dialogfeld **Content Control List – Verwaltung** eine CCL aus und klicken Sie auf **OK**.
6. Klicken Sie im Bereich **Regelinhalt** auf den Link **Ziel auswählen** und aktivieren Sie die Option **Wechselspeicher**. Klicken Sie auf **OK**.
7. Wählen Sie im Dialogfeld **Verwaltung der Data Control-Regeln** die erstellte Regel aus und klicken Sie auf **OK**.
8. Schließen Sie alle Dialogfelder und übertragen Sie die Richtlinie auf die Testcomputer.

## 6.2 Überprüfen der Funktionalität von Data Control

1. Öffnen Sie **Sophos Endpoint Security and Control** auf den Testcomputern.
2. Überprüfen Sie im **Status**-Feld auf der Startseite, ob Data Control aktiviert ist.
3. Klicken Sie auf das **Data Control-Protokoll**-Symbol. Überprüfen Sie, ob der Data Control-Scanvorgang gestartet wurde.

## 7 Testen von Device Control

### 7.1 Konfigurieren von Device Control

1. Öffnen Sie in Enterprise Console eine Application Control-Richtlinie.
2. Konfigurieren Sie die Richtlinie so, dass **Modems** und **Wireless**-Geräte gesperrt werden.  
In den Computerdetails sollte in der Spalte zur Konformität mit der Device Control-Richtlinie „Richtlinienübertragung wird erwartet“ und „Wie Richtlinie“ stehen.
3. Übertragen Sie die Richtlinie auf die Testcomputer.
4. Überprüfen Sie, ob der Endpoint jetzt mit der Richtlinie konform ist.

### 7.2 Überprüfen der Funktionalität von Device Control

1. Schließen Sie an die Endpoints, Modems und Wireless-Geräte an.  
Zu allen gesperrten Geräten sollte eine Sprechblasenmeldung angezeigt werden.
2. Öffnen Sie Sophos Endpoint Security and Control. Klicken Sie auf der Startseite auf das **Device Control-Protokoll** und stellen Sie sicher, dass das Gerät gesperrt wurde.
3. Überprüfen Sie im Windows Geräte-Manager, ob das Gerät deaktiviert wurde.

4. Versuchen Sie, mit dem Wireless-Gerät eine Verbindung zu einem Wireless-Netzwerk herzustellen.

Windows sollte nun anzeigen, dass das Gerät gesperrt wurde und keine Netzwerke erkennen kann.

5. Versuchen Sie, das Modem mit dem Windows Geräte-Manager zu testen. Überprüfen Sie, ob das Modem nicht getestet werden kann.

### 7.3 Zurücksetzen der Device Control-Richtlinie

1. Konfigurieren Sie die Device Control-Richtlinie in Enterprise Console wie folgt:

- Modem: Vollzugriff.
- Wireless: Vollzugriff.

2. Übertragen Sie die Richtlinie auf die Testcomputer.
3. Überprüfen Sie, ob die Computer mit der Richtlinie konform sind.
4. Klicken Sie auf den Testcomputern auf das **Device Control-Protokoll**-Symbol und stellen Sie sicher, dass das Gerät aktiviert ist.
5. Überprüfen Sie, ob das Wireless-Gerät Wireless-Netzwerke erkennen kann.
6. Versuchen Sie, das Modem mit dem Windows Geräte-Manager zu testen. Überprüfen Sie, ob der Geräteselbsttest erfolgreich ist.

## 8 Copyright

Copyright © 2009 Sophos Group. 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 Plc und der Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to [support@sophos.com](mailto:support@sophos.com) 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>