Ersteller/Editor	Ulrike Hirtreiter	Änderungsdatum	40.07.2021
Erstellungsdatum	06.07.2012	Status	Final

Sophos Virenscanner

Konfiguration

Inhaltsverzeichnis

1. Vorwort 3
2. Sophos Endpoint Security and Control - Konfiguration 4
2.1 AntiVirus 4
2.1.1 On-Access-Scans 4
2.1.2 Verhaltensüberwachung 4
2.1.3 Erweiterungen und Ausschlüsse für On-Demand-Scans 4
2.1.5 Rechtsklick-Scans (auch „On Demand Scans“) 5
2.1.6 Sophos Live Schutz 5
2.1.7 Webschutz 5
2.1.8 Autorisierung 5
2.1.9 Benutzerrechte für Quarantäne-Manager 5
2.1.10 Benachrichtigungen 5
2.1.12 Protokoll 6
2.2 Application Control 6
2.3 Benutzer authentifizieren 6
2.4 Manipulationsschutz 6
2.5 Web Control 6
2.6 Exploit Abwehr 6
2.7 Updates 6
3. Glossar 7

1. Vorwort

Das Rechenzentrum betreibt für alle dienstlichen Computer einen Sophos Server, der als zentrale Basisstation allen Clients die neuesten Updates zur Verfügung stellt und über den die RZ-Standard-Konfiguration des Virenscanners verwaltet wird. Im Folgenden finden Sie einen kurzen Überblick über die Konfiguration des Client-Virenscanners.

2. Sophos Endpoint Security and Control - Konfiguration

Der Client-Virenscanner von Sophos heißt „Sophos Endpoint Security and Control“, da das Produkt mehr Funktionen als den reinen Virenschutz bietet. Im Uni-Jargon wird üblicherweise immer von Sophos Anti-Virus gesprochen.

Im Folgenden finden Sie die wichtigsten RZ-Standard-Einstellungen kurz erläutert.

2.1 AntiVirus

2.1.1 On-Access-Scans

a. Scanning

- aktiv: Dateien werden beim Lesen, Schreiben und Umbenennen gescannt
  Beim Versuch, eine Datei zu kopieren, zu verschieben, zu verändern oder zu öffnen, scannt Sophos Anti-Virus die Datei (auch solche ohne Dateierweiterung). Der Zugriff wird nur erlaubt, wenn die Datei frei von Schadcode ist bzw. zugelassen wurde.
- aktiv: Scannen auf Adware (Werbung) und PUA (potenziell unerwünschte Anwendung)
- inaktiv:
  verdächtige Dateien
  Zugriff auf Laufwerke mit infiziertem Bootsektor erlauben
  „Archivdateien scannen“ und „Alle Dateien scannen“ aus Performancegründen

b. Bereinigung
Aktiv: nur Zugriff verweigern

- Die automatische Bereinigung ist nicht aktiv, da diese fälschlicherweise zur Bereinigung einer Datei führen kann und diese dadurch u. U. unbenutzbar wird.
- Wenn nicht bereinigt werden kann oder eine Datei verdächtig erscheint wird automatisch der Zugriff auf die Datei verweigert und eine Kopie der Datei in die Quarantäne gelegt.

2.1.2 Verhaltensüberwachung

Aktiv (alle Optionen)

Die Erkennung verdächtigen Verhaltens führt mit Hilfe von Sophos HIPS (Host Intrusion Prevention System) eine dynamische Verhaltensanalyse aller auf dem Computer ausgeführten Programme durch, um Aktivitäten zu erkennen und zu sperren, die wahrscheinlich schädlich sind. Zu verdächtigem Verhalten zählen beispielsweise Änderungen an der Windows Registry, die das automatische Ausführen eines Virus zulassen, wenn der Computer neu gestartet wird. Auch Pufferüberlauf-Attacken auf laufende Prozesse werden erkannt. Dadurch erhöht sich der Schutz für die Rechner, da Code noch vor der Ausführung analysiert wird und bei Einstufung als verdächtig oder schädlich nicht ausgeführt wird. Außerdem stoppt die Laufzeiterkennung Bedrohungen, die vor der Ausführung nicht erkannt werden können.

2.1.3 Erweiterungen und Ausschlüsse für On-Demand-Scans

Hier findet man eine Liste von zu scannenden Dateiformaten bei On-Demand-Scans. Auch Dateien ohne Dateierweiterung werden gescannt.

2.1.5 Rechtsklick-Scans (auch „On Demand Scans“)

a. Scannen

- aktiv:
  Adware und PUA, Archivdateien scannen, Alle Dateien scannen

b. Bereinigung

- Die automatische Bereinigung ist nicht aktiv, da diese fälschlicherweise zur Bereinigung einer Datei führen kann und diese dadurch u. U. unbenutzbar wird.
- Wenn nicht bereinigt werden kann oder eine Datei verdächtig erscheint wird automatisch ein Eintrag im Protokoll erstellt.

Diese Einstellungen sind mit Benutzerrechten am Client durch jeden Anwender änderbar!!

2.1.6 Sophos Live Schutz

Aktiv

Der Live-Schutz bestimmt, ob es sich bei einer verdächtigen Datei um eine Bedrohung handelt. Wenn der Live Schutz aktiv ist, werden bestimmte Dateidaten (z.B. die Prüfsumme der Datei und weitere Attribute) zur weiteren Analyse an Sophos übermittelt. Dies erfolgt aber nicht automatisch, sondern nur nach Meldung und Bestätigung durch den User. Dies ist immer dann der Fall, wenn eine Datei auf einem Client von Sophos als verdächtig eingestuft wurde, aber er sich nicht sicher ist, ob die Datei wirklich virenfrei ist.

2.1.7 Webschutz

Aktiv: Zugriff auf schädliche Websites sperren
für Downloads gelten die Vorgaben, die im On-Access-Scan definiert wurden

2.1.8 Autorisierung

nichts konfiguriert

Wenn Sie Adware, eine Anwendung oder ein Objekt ausführen möchten, das von Sophos als potenziell unerwünscht klassifiziert wurde, können Sie diese hier zulassen.

2.1.9 Benutzerrechte für Quarantäne-Manager

Wird ein Objekt von Sophos in die Quarantäne verschoben, so haben nur der sog. Sophos Administrator und der Power User (im Default alle Administratoren am Client) Zugriff darauf, der normale Benutzer kann keine Aktionen für Objekte in der Quarantäne durchführen. Ein Sophos Administrator oder Power User kann Objekte aus der Quarantäne löschen oder eine Bereinigung einer Datei in der Quarantäne anstoßen.

2.1.10 Benachrichtigungen

Alle Desktop-Benachrichtigungen sind aktiviert. Dies bedeutet, dass jeder Anwender durch eine Meldung am Bildschirm informiert wird, wenn Sophos eine Datei als schädlich identifiziert. Außerdem erfolgt eine Ereignisprotokollierung bei diesen Ereignissen: Erkennen von Spyware und Viren, Erkennen verdächtigen Verhaltens und verdächtiger Dateien, Adware und PUA Erkennung und -Bereinigung, Sonstige Fehler

Alle E-Mail- Benachrichtigungen sind aktiviert. Dies bedeutet, dass alle Meldungen von Sophos an eine zentrale Mail-Adresse der UR gesendet werden.

Ereignisprotokollierung ist aktiv.

2.1.12 Protokoll

Die normale Protokollierung mit monatlicher Archivierung des Protokolls (4 Monate zurück) ist aktiv. Das Protokoll wird komprimiert und lokal auf dem Rechner abgelegt.

Bei Auswahl der Option „Normal“ werden Zusammenfassungen, Fehlermeldungen usw. protokolliert. Klicken Sie auf der Startseite in Sophos unter „Antivirus und HIPS“ auf „Antivirus- und HIPS-Protokoll anzeigen“, um das Protokoll zu öffnen.

2.2 Application Control

Inaktiv
Mit dieser Funktion könnte die Nutzung von bestimmten Programmen am Client erlaubt oder verhindert werden.

2.3 Benutzer authentifizieren

Inaktiv
Nur in Verbindung mit der Funktion „Manipulationsschutz“ nutzbar!

2.4 Manipulationsschutz

Inaktiv
Mit dem Manipulationsschutz können Sie u.a. verhindern, dass nicht autorisierte Benutzer, die über Admin-Rechte am Client verfügen, Sophos deinstallieren. Aufgrund der ohnehin sehr hohen Sensibilisierung der Anwender bzgl. Virenschutz an der Universität ist diese Funktion nicht aktiv.

2.5 Web Control

Inaktiv

Damit kann z.B. der Aufruf unangebrachter Websites kontrolliert werden.

2.6 Exploit Abwehr

Aktiv

Die Exploit Abwehr von Sophos bietet:

- Schutz von Dokumenten vor Ransomware (CryptoGuard).
- Schutz vor Angriffen auf den Bootsektor (WipeGuard).
- Schutz kritischer Funktionen in Webbrowsern (sicheres Surfen).
- Abschwächung von Exploits. Damit werden Anwendungen geschützt, die besonders anfällig für Malware-Exploits sind, wie z. B. Java-Anwendungen.
- Schutz vor schwächenden Angriffen auf Prozesse.
- Schutz vor einem Laden von .DLL-Dateien aus nicht vertrauenswürdigen Verzeichnissen.
- Schutz vor einer Nachverfolgung der Prozessor-Verzweigungen.

2.7 Updates

Immer 5-10 min nach dem Boot des Rechners nimmt Sophos Kontakt zum RZ Sophos Server auf. Darüber hinaus verbindet sich ein aktiver Client automatisch alle 60 min mit dem RZ Sophos Server zur Überprüfung auf neue Updates.

Hinweis:
Die oben beschriebene Konfiguration des Client-Virenscanners kann mit administrativen Rechten am Client verändert werden über das „Sophos Endpoint and Security-Menü“ „Konfigurieren“.

3. Glossar

a. On Access Scan
   Dateien werden automatisch auf Viren überprüft, sobald sie vom Benutzer verwendet (geöffnet oder gespeichert) werden.

b. On Demand Scan
   Das Scannen von Files erfolgt nicht automatisch, sondern wird durch den Anwender veranlasst.