Creator/Editor	Ulrike Hirtreiter	Modification Date	23.09.2021
Creation date	06.07.2012	State	Final

Sophos Virus Protection

Configuration

Table of contents

1. Introduction

The data center operates a Sophos server for all business computers which, as a central base station, provides all clients with the latest updates and which is used to manage the standard data center configuration of the virus scanner. The following is a brief overview of the configuration of the client virus scanner.

2. Sophos Endpoint Security and Control - Configuration

The Sophos client virus scanner is called "Sophos Endpoint Security and Control" because the product offers more functions than just virus protection. The term Sophos Anti-Virus is usually used in university jargon.

The most important data center standard settings are briefly explained below.

2.1 AntiVirus

2.1.1 On-Access-Scans

a. Scanning

- active: files are scanned during reading, writing and renaming
  When you try to copy, move, modify or open a file, Sophos Anti-Virus scans the file (even those without a file extension). Access is only permitted if the file is free of malicious code or has been approved.
- active: scanning for adware (advertising) and PUA (potentially unwanted application)
- inactive:
  suspicious files

  Allow access to drives with an infected boot sector

  "Scan archive files" and "Scan all files" for performance reasons

b. Cleanup

Active: deny access only

- Automatic cleanup is not active, as it can erroneously clean up a file, which may make it unusable.
- If a file cannot be cleaned or a file appears suspicious, access to the file is automatically denied and a copy of the file is placed in the quarantine.

2.1.2 Behavioral monitoring

Active (all options)

Suspicious behavior detection uses Sophos HIPS (Host Intrusion Prevention System) to dynamically analyze the behavior of all programs running on the computer to identify and block activities that are likely to be harmful. Suspicious behavior includes changes to the Windows registry that allow a virus to run automatically when the computer is restarted. Buffer overflow attacks on running processes are also detected. This increases the protection for the computers, since code is analyzed before it is executed and, if it is classified as suspicious or harmful, will not be executed. Also, runtime detection stops threats that cannot be detected before execution.

2.1.3 Enhancements and Exclusions for On-Demand Scanning

Here is a list of the file formats to be scanned for on-demand scans. Files without a file extension are also scanned.

2.1.5 Right-click scans (also "On Demand Scans")

a. Scanning

- active:
  Adware and PUA, scanning archive files, scanning all files

b. Cleanup

- Automatic cleanup is not active, as it can erroneously clean up a file, which may make it unusable.
- If it cannot be cleaned or a file appears suspicious, an entry is automatically created in the log.Diese Einstellungen sind mit Benutzerrechten am Client durch jeden Anwender änderbar!!

2.1.6 Sophos Live Protection

Active

Live protection determines whether a suspicious file is a threat. When live protection is active, certain file data (e.g. the file's checksum and other attributes) are sent to Sophos for further analysis. However, this does not happen automatically, but only after notification and confirmation by the user. This is always the case when a file has been classified as suspicious on a Sophos client, but it is not sure whether the file is really virus-free.

2.1.7 Web protection

Active: Block access to malicious websites

the specifications defined in the on-access scan apply to downloads

2.1.8 Authorization

nothing configured

If you want to run adware, an application, or an item that Sophos has classified as potentially unwanted, you can allow it here.

2.1.9 Quarantine Manager user rights

If an object is quarantined by Sophos, only the so-called Sophos administrator and the power user (by default all administrators on the client) have access to it, the normal user cannot perform any actions on objects in the quarantine. A Sophos administrator or power user can delete objects from quarantine or initiate a cleanup of a file in quarantine.

2.1.10 Notifications

All desktop notifications are enabled. This means that every user is informed by an on-screen message when Sophos identifies a file as malicious. Events are also logged for these events: spyware and virus detection, suspicious behavior and files detection, adware and PUA detection and cleanup, other errors

All email notifications are enabled. This means that all reports from Sophos are sent to a central email address in the UR.

Event logging is active.

2.1.11 Protocol

The normal logging with monthly archiving of the log (4 months back) is active. The log is compressed and stored locally on the computer.

If you select the "Normal" option, summaries, error messages, etc. are logged. On the Sophos Home page, under Antivirus and HIPS, click View Antivirus and HIPS Log to open the log.

2.2 Application Control

Not active
With this function, the use of certain programs on the client could be allowed or prevented.

2.3 Authenticate users

Not active
Can only be used in conjunction with the "Tamper protection" function!

2.4 Tamper protection

Not active
With tamper protection, you can prevent unauthorized users who have admin rights on the client from uninstalling Sophos. Due to the already high level of user awareness regarding virus protection at the university, this function is not active.

2.5 Web Control

Not active

This can be used, for example, to control calls to inappropriate websites.

2.6 Exploit Prevention

Active

Sophos's exploit defense offers:

- Protection of documents against ransomware (CryptoGuard).
- Protection against attacks on the boot sector (WipeGuard).
- Protection of critical functions in web browsers (safe surfing).
- Mitigation of exploits. This protects applications that are particularly vulnerable to malware exploits, such as: B. Java applications.
- Protection against debilitating attacks on processes.
- Protection against loading .DLL files from untrustworthy directories.
- Protection against tracing of the processor branches.

2.7 Updating

Sophos contacts the data center Sophos server 5-10 minutes after the computer has booted. In addition, an active client automatically connects to the RZ Sophos server every 60 minutes to check for new updates.

Note:
The configuration of the client virus scanner described above can be changed with administrative rights on the client via the "Sophos Endpoint and Security menu" "Configure".

3. Glossary

a. On Access Scan
   Files are automatically scanned for viruses as soon as they are used (opened or saved) by the user.

b. On Demand Scan
   The scanning of files does not take place automatically, but is initiated by the user.