Virenschutz

Virenschutz

- Überblick
- Anleitung
- Download/Links

Grundschutz für Rechner

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) hat auf seinen Internetseiten wichtige Hinweise zusammengestellt, um Rechner vor schädlichen Angriffen zu schützen. Detaillierte Informationen finden Sie auf dieser Seite des BSI.

Einer der wichtigen Hinweise, ist der Einsatz von Antivirensoftware.

Antivirensoftware

Zum Schutz vor Schadprogrammen wie Viren, Trojaner, Würmer und Co wird vorgeschrieben eine Antivirensoftware einzusetzen. In der Regel besteht diese aus einem Virenscanner/manuellen Scanner und einem Virenwächter/Echtzeitscanner.

Auf Rechnern der Hochschule (Dienstgeräte) kann die Antivirensoftware von Sophos installiert werden. Damit erhalten Rechner der Hochschule mit all den anderen vom BSI empfohlenen Maßnahmen ein Mindestmaß an Schutz vor Schadprogrammen.

Auf den Rechnern, mit den Betriebssystemen Windows, Mac OS X und Linux, bei Sophos Endpoints genannt, wird das Produkt "Sophos Endpoint Security and Control" installiert, auch kurz Sophos Anti-Virus genannt.

Das RZ betreibt einen Sophos Management Server (Sophos Enterprise Console), welcher die Endpoints mit der Grundkonfiguration des Antivirenprogramms, Standardrichtlinien, Antivirendefinitionsupdates und Engine-Updates versorgt.

Sophos Anti-Virus unterstützt die Windows Betriebssysteme Windows 7, Windows 8, Windows 8.1 und Windows 10.

Ebenfalls werden auch die Windows Server-Betriebssysteme Windows Server 2008, Windows Server 2012 und Windows Server 2016 unterstützt.

Die Offizielle Windows XP Unterstützung von Sophos ist ausgelaufen. Ebenfalls ist zu beachten das Windows XP Rechner keinerlei Support und Updates von Microsoft mehr bekommen und müssen daher zeitnah stillgelegt werden.

Das aktuelle Sophos Anti-Virus wird von der Hochschule Offenburg über den Sophos Management Server zur Verfügung gestellt. In den jeweiligen Anleitungen für Windows, Mac OS X und Linux ist beschrieben, wie die Software installiert wird.

Anleitung für Windows

Installation von Sophos Anti-Virus auf Windows-Rechnern im Hochschulnetz und Rechnern mit VPN-Verbindung ins Hochschulnetz

1. Kopieren der Installations-Datei von Sophos Anti-Virus

Auf dem Netzwerklaufwerk I: findet man im Verzeichnis I:\inst\sophos die Datei ***SophosEndpoint_RMS.v5.5.exe***, diese Datei kopieren Sie einfach auf Ihren PC.

Falls der Rechner keinen OES Client installiert hat für die Netzlaufwerke, können Sie auch über FILR auf die Datei zugreifen (mehr dazu in dem Tab: Download/Links).

2. Ausführen der Installations-Datei vom lokalen Laufwerk

Die Installations-Datei per Rechts-Klick auswählen und "Als Administrator ausführen" auswählen.
Danach startet das Setup-Programm die Sophos Anti-Virus Installation und führt Sie durch die Installation.

3. Überprüfung der Installation

In der Taskleiste unten rechts in der Nähe der Uhrzeit erscheint ein Schutzschild mit einem S (Sophos-Symbol). Daran ist zu erkennen, dass Sophos Anti-Virus korrekt installiert ist.
Direkt nach der Installation werden im Hintergrund die neuesten Antivirendefinitionsdateien heruntergeladen. Es dauert ein paar Minuten und dann kann per Rechts-Klick auf das Sophos-Symbol das Programm Sophos Endpoint Security and Control gestartet werden.
Dort wird das Datum und die Uhrzeit des letzten Updates angezeigt.
Bitte kontrollieren Sie, ob regelmäßige Updates heruntergeladen werden.

Nach oben

Anleitung für Linux

Führen Sie die Installationsschritte mit root-Rechten aus.

1. Firewall-Freischaltung für Sophos-Server

Damit Sophos Anti-Virus Konfigurationseinstellungen vom zentralen Management-Server bekommen kann, muss der Rechner sich in einem der Nichtöffentlichen Netzen befinden, und Port TCP/8194 muss für Zugriff von 141.79.128.45 freigeschaltet werden.

Ohne diese Freischaltung bekommt Sophos-Antivirus nicht die Informationen über die Update-Quellen.

2. Installationslaufwerk vom Sophos-Server mounten, z.B.:

mount //141.79.128.45/SophosUpdate /mnt

Es ist keine Anmeldung erforderlich. Zugriff nur von den "Nichtöffentlichen Netzen" bzw. über VPN.

3. Ins Installationsverzeichnis wechseln:

cd /mnt/CIDs/S000/savlinux/

4. Installationsskript mit Parametern ausführen:

./install.sh /opt/sophos-av --automatic --acceptlicence --update-source-path=\\sec.rz.hs-offenburg.de\sophosupdate\cids\s000\savlinux --update-source-type=o --sec-group="\sec.rz.hs-offenburg.de\Default"

Alternativ kann ./install.sh ohne Parameter aufgerufen werden und die Informationen interaktiv angegeben werden.

5. Nutzung der Kommandozeile:

Hinweis: Das in einer früheren Version dieser Anleitung beschriebene Web-GUI steht nicht mehr zur Verfügung. Sophos schreibt dazu:

https://community.sophos.com/kb/en-us/122722 : "From SAV Linux 9.11.0 the web GUI will no longer be a feature of SAV for LINUX. Locally, this will now be entirely controlled from the command line."

Zur Kontrolle von Sophos-AV stehen unter /opt/sophos-av/bin einige Kommandozeilen-Programme zur Verfügung: savconfig, savdctl, savdstatus, savlog, savscan, savsetup, savupdate

Weitere Informationen wie unter Linux üblich mit --help und man. Deinstallation der Linux-Version:/opt/sophos/uninstall.sh

6. Updates

Sophos Anti-Virus sollte alle 10 Minuten (*) auf dem Server nach neuen Updates schauen. Sofern sich der Rechner in den "Nichtöffentlichen Netzen" der Hochschule befindet bzw. eine VPN-Verbindung hat, werden die Updates vom Management-Server des RZ bezogen. Scheitert dieser Zugriff werden die Updates direkt von Sophos geholt. Überprüfen Sie ab und zu, ob sich Ihr System noch erfolgreich die Updates holt - Virenscanner ohne Updates sind nahezu sinnlos!

(*) Die 10 Minuten sind der derzeit auf dem zentralen Sophos-Server des RZ eingestellte Wert - dieser kann sich ändern.

Zur Kontrolle, ob Updates erfolgreich laufen, können Sie das Programm savlog verwenden - Beispiel:

hrz-99:/opt/sophos-av/bin # ./savlog | grep update

[..]

Fri Oct 7 09:33:37 2016: update.updated Updating from versions - SAV: 9.12.0, Engine: 3.64.3, Data: 5.30
Fri Oct 7 09:33:37 2016: update.updated Updating Sophos Anti-Virus....
Fri Oct 7 09:33:37 2016: update.updated Updated to versions - SAV: 9.12.2, Engine: 3.65.2, Data: 5.32
Fri Oct 7 09:33:37 2016: update.updated Successfully updated Sophos Anti-Virus from \\sec.rz.hs-offenburg.de\SophosUpdate\CIDs\S000\savlinux

Informationen über die Update-Quellen sehen Sie mit savconfig:

```
hrz-99:/opt/sophos-av/bin # ./savconfig query
AllowIfBootSectorThreat: false
AutomaticAction: disinfect
EmailDemandSummaryIfThreat: true
EmailLanguage: english
EmailNotifier: false
EnableOnStart: true
ExclusionEncodings: UTF-8
        EUC-JP
        ISO-8859-1
LogMaxSizeMB: 100
NotifyOnUpdate: false
PrimaryUpdateSourcePath (Locked): \\sec.rz.hs-offenburg.de\SophosUpdate\CIDs\S000\savlinux
PrimaryUpdateUsername (Locked): SEC\SophosUpdateMgr
PrimaryUpdatePassword (Locked): ********
SecondaryUpdateSourcePath (Locked): sophos:
```

SecondaryUpdateUsername (Locked): 2ODXRBOVCU
SecondaryUpdatePassword (Locked): ********
UploadSamples: false
SendErrorEmail: false
SendThreatEmail: false
UINotifier: true
UIpopupNotification: true
UIttyNotification: true
UpdatePeriodMinutes (Locked): 10
NamedScans: SEC:FullSystemScan [Not scheduled]
LiveProtection: enabled
ScanArchives: disabled

Ein manuelles Update können Sie mit savupdate auslösen:

hrz-99:/opt/sophos-av/bin # ./savupdate
Successfully updated Sophos Anti-Virus from \\sec.rz.hs-offenburg.de\SophosUpdate\CIDs\S000\savlinux

7. Deinstallation

Zur Deinstallation unter /opt/sophos-av das Skript uninstall.sh ausführen.

8 Weitere Informationen

Beachten Sie auch die Links auf die Systemvorraussetzung und die Dokumentation vom Hersteller im Tab "Downloads/Links"

Anleitung für Mac OS X

Anleitung für Mac OS X herunterladen [PDF]

Sophos Installationsanleitungen

Anleitungen für

- Windows (bitte verwenden Sie die Datei *SophosEndpoint_RMS.v5.5.exe*)
- Macintosh
- Linux
  - Kurzanleitung siehe im Tab "Anleitung" und im Installationsverzeichnis untem
  - Dokumentation des Herstellers: https://www.sophos.com/en-us/support/documentation/sophos-anti-virus-for-

linux.aspx?platform=Version-9#Version-9

- Systemvoraussetzungen: https://community.sophos.com/kb/en-us/14377

Installationsverzeichnis mit Anleitungen und Installationsdatei:

Mit Novell Client:	I:\inst\sophos
über CIFS/SMB:	\\fs1-2-common.rz.hs-offenburg.de\common\inst\sophos
Filr:	https://filr.hs-offenburg.de -> Netzwerkordner -> inst -> sophos
Dateiname:	*SophosEndpoint_RMS.v5.5.exe* **Bitte verwenden Sie die veraltete Batch-Datei nicht mehr!**