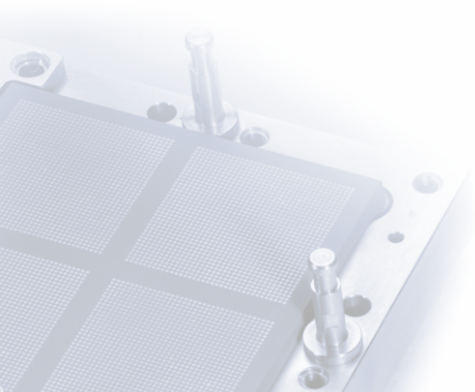


Sophos Endpoint-Security

Hergen Harnisch
harnisch@rrzn.uni-hannover.de



Server-Setup

Clients:

Windows

Linux/Unix

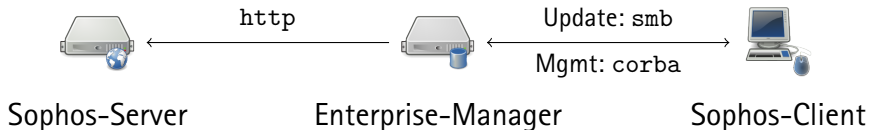
andere

Aktuelles:

Shh/Updater-B

Sophail

Sophos-Standard



- Updates via http von Sophos-Servern, über Share innerhalb Org.
 - Management von Clients (RMS) in beide Richtungen
 - EM und Clients in einem Active-Directory, häufig auch RPC-Zugriff als Administrator durch EM
- Das meist Grundlage der Dokumentationen durch Sophos.

Sophos-Standard vs. LUH

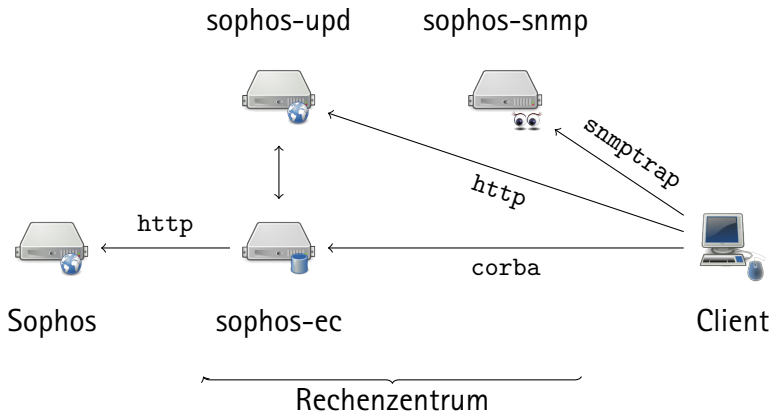
Das Setup funktioniert nicht für uns:

- keine gemeinsame AD-Struktur
 - Zentrale Domäne existiert (noch?) nicht, würde nicht alle Clients abdecken.
 - Vertrauensstellungen sind ein Sicherheitsproblem.
- keine zentrale Admin-Berechtigung über Clients
- Shares gehen bewusst nicht über LAN-Grenzen (ACLs)
- Firewalling verhindert RMS-Zugriff EM auf Client: Netzschutz, Personal-FW der Clients
- Notebooks so nicht unterstützt.

Anforderungen in der LUH

- Unabhängigkeit von Windows-Domänen-Strukturen
- Updatefähigkeit aus dem Internet, Funktionsfähigkeit über interne Firewalls
- zentrales Reporting
- heterogene Policies
- wenige, zentrale Server

LUH-zentral: Überblick



LUH-zentral: Server

`sophos-upd` über `http` erreichbare Update-Server

- z.T. unter Linux, authentifiziert auch aus dem Internet
- enthält verschiedene Zweige mit verschiedenen Policies

`sophos-ec` über Sophos-RMS erreichbarer Verwaltungs-Server


- windows-basiert, zieht die Updates von Sophos
- versorgt `sophos-upd` mit aktualisierten Dateien & Policies
- Enterprise-Manager zum Verwalten von Clients & Policies
- erreichbar nur aus dem LUH-Netz






`sophos-snmp` SNMP-Trap-Receiver (nur aus LUH-Netz)

- empfängt Fehler- und Alarm-Meldungen der Sophos-Clients

Zum Teil sind es die gleichen Server-Installationen.

Enterprise-Manager

Ansicht:  Alle Computer Diese Ebene und abwärts

Status	Computer-Details	Update-Details	Alert- und Fehlerdetails	Antivirus-Details	Firewall-Details	NAC-Details	Application Control	Data Control	Device Control	Manipulationsschutz
	Computernamen	Richtlinienkonformität	Auf dem neuesten Stand	Alerts und Fehler	On-Access	Fir				
	PC_503030		Ja		Aktiv					
	PC_54F7F4		 Nicht seit 16.11.2012 18:56:47		Aktiv					
	PC_A76198		 Nicht seit 16.11.2012 18:56:47		Aktiv					
	PC_DELL_32354A		 Nicht seit 16.11.2012 21:36:49	 Adware/PUA erkannt	Aktiv					
	PC_#####		 Nicht seit 16.11.2012 17:27:26		Aktiv					

Möglichkeiten durch Enterprise-Manger & RMS-Anbindung:

- Client-Status, -Fehler, -Alarme in EM-GUI & -DB
- teilweise Bereinigen der Infektionen
- Ausrollen von Policies (überschreibt lokale Einstellungen in Teilen)

Ausstehende Alerts und Fehler

Objekte erkannt


Zuerst erkannt am/um	Typ	Bereinigungsstatus	Name	Subtyp	Details	Dateiversion
15.11.2012 14:53:27	Virus/Spyware	Keine Bereinigung möglich	ShhUpdater-B		C:\Programme\Adobe\Acrobat 8.0\Acrobatplug_ins\updater.DEU	

Verlauf

Objekte erkannt

Zeitstempel	Typ	Name	Subtyp	Details	Dateiversion	Maßnahme	Benutzername
15.11.2012 14:53:27	Virus/Spyware	ShhUpdater-B		C:\Programme\Adobe\Acrobat 8.0\Acrobatplug_ins\updater.DEU		Gesperrt	

Name & Beschreibung

Ansicht:  Alle Computer		Diese Ebene und abwärts		
Status Computer-Details Update-Details Alert- und Fehlerdetails Antivirus-Details Firewall-Details NAC-Details Application Control Data Control Device Control Manipulationsschutz				
Computername	Computerbeschreibung	Betriebssystem	Service P...	Domäne/Arbeits...
PC_503030	746B8159-A789-E011-ABDD-505054503030;;;E0:69:55:00:00:00;20110928	Windows XP (64 Bit)	Service P...	
PC_54F7F4	1E00F640-008C-E200-4525-BCAEC554F7F4;;;130.75.100.100;BC:AE:00:00:00:00;20111028	Windows XP (64 Bit)	Service P...	
PC_A76198	00000000-0000-0000-0000-1C6F65A76198;;;130.75.100.100;1C:6F:00:00:00:00;20121017	Windows 7	Service P...	
PC_DELL_32354A	4C4C4544-0051-5110-8037-C6C04F32354A;;;20111010	Windows 7	Service P...	
PC_888888	FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFFFF;00:14:00:00:00:00;20110412	Windows 7 (64 Bit)	Service P...	

Damit PCs zugeordnet werden können und Namen eindeutig sind:

- LUH-SAU-Installer (managed) überschreibt

Computer-Namen & Beschreibung

- Name ist Computername, ggf. ergänzt um UUID-Teil
- Beschreibung enthält
 - System-UUID & WSUS-UUID
 - LUH-IP-Adressen während der Installation, MAC-Adresse

→ Nur automatischen Installer für gemanagte Clients verwenden!

... trotzdem bleibt Client-Identifikation schwierig.

SNMP-Reporting

```
20121116-1619.12 130.75.xx.yy 130.75.xx.yy  
10.0.9 (26816821) 3 days, 2\x3a29\x3a28.21 virus  
Datei \"C\x3a\\Users\\...\\Keygen.exe\"  
geh\x3c3\xb6rt zu Virus/Spyware 'Mal/KeyGen-M'.  
20121116-1619.14 130.75.xx.yy 10.5.47.11  
10.0.8 (17461546) 2 days, 0\x3a30\x3a15.46 virus  
Virus/spyware 'Shh/Updater-B' has been detected in
```

```
\\\"C\x3a\\Program Files (x86)\\Secunia\\PSI\\sua.exe\".\r\n
```

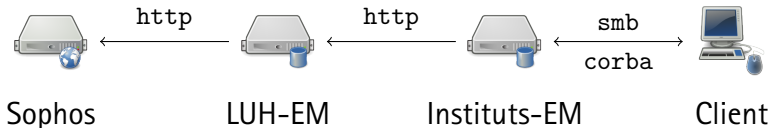
bisher SNMP-Trap-Empfang in zentrale Logs

geplant über DB strukturierte Auswertung & Reporting an Institute

Probleme Parsing der SNMP-Meldungen fast unmöglich:

- Sophos nutzt Strukturierungsmöglichkeiten von SNMP nur sehr wenig.
- Sophos übersetzt auch die in SNMP-Traps enthaltene Strings.
- Das Escaping der Strings ist client-seitig unterschiedlich.

einrichtungseigene EM



- kaskadiert an LUH-Enterprise-Manager
- Setup des Instituts-EM ist (fast) Sophos-Standard
- kein Support, nur wenig Rücksicht darauf möglich
→ *bitte bei uns EM-Einsatz anzeigen, auch bisherige*
- *nicht empfohlen, nur noch wenige Vorteile*

LUH-Installer

	außerhalb LUH	RMS-Funktion	SNMP-Reporting
home	X		
managed	X	X	X
unmanaged	X		X

home Für die zugelassene Privatnutzung auf Nicht-LUH-PCs

managed Computer-Name und Computer-Beschreibung werden vom LUH-Installer speziell angepasst, empfohlen für alle normalen Clients (Server, Desktops, Notebooks).

unmanaged gedacht für geclonte Clients; nötig, da beim Cloning Sophos-Client-ID mehrfach auftaucht und dadurch RMS unmöglich wird

neue Features



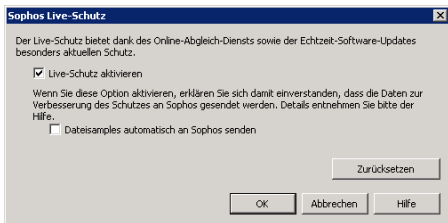
- Live-Schutz
- Web-Schutz
- Web-Control
- Manipulationsschutz

Live-Schutz

Dateien mit Malware oder verdächtigem Verhalten werden bei Sophos angefragt:

- Nicht Datei, sondern Hash mit weiteren Meta-Daten
- Antwort informiert Clients, ob Malware bekannt.
- Zusätzlich kann man einer automatischen Sample-Übermittlung an Sophos zustimmen.

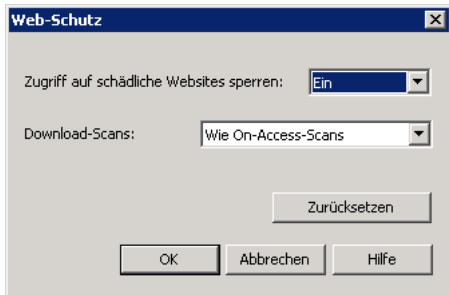
Wohl per DNS, Genauer Satz Daten bei Übermittlung unklar.



Web-Schutz

Verhindert den Zugriff auf bösartige Webseiten.

- Statt Webseite wird SAV-Info-Seite im Browser angezeigt.
- Abfrage erfolgt live bei Sophos via DNS-Anfragen:
sybjpnfgfzrqvn.ryrneavat.hav-unaabire.qr.u.04.s.sophosxl.net IN TXT
- „auf der zentralen Sophos Datenbank werden Anfragen nicht ausgewertet“



Version 7.5

Bietet On-Access-Scanning und kann verwaltet werden.

- installiert sich mit init-Skripten
- startet Dienste („Loopback-Webserver“ als GUI)
- lädt Kernel-Modul
 - „talpa“ ist Sophos-Entwicklung, nicht im Standard-Kernel
 - Version muss passen, ggf. erst kompiliert werden
 - auch bei unterstützten Distributionen kann Unterstützung nach Kernelupdate hinterherhängen
 - unterstützt sind z.B. Ubuntu-LTS-Versionen, Debian nicht; vgl. http://sophosupd1.rrzn.uni-hannover.de/SophosUpdate/CIDs/S000/savlinux/supported_kernels.txt

—> von uns nicht empfohlen, nicht supportet

Installer unter <http://www.rrzn.uni-hannover.de/fileadmin/SOPHOS/sav-linux-7-i386.tgz>

Update-Pfad <http://sophosupd?.rrzn.uni-hannover.de/SophosUpdate/CIDs/S00/?savlinux>

Version 4

- bietet kein On-Access-Scanning, nur On-Demand-Scanning
- nachwievor aktuell und mit Virensignaturen beliefert
- geht hauptsächlich um Windows- oder Mac-Malware
- sinnvoller Einsatz:
 - Scanner für Linux-Boot-CD („Rescue-CD“)
 - bei Bedarf in Linux-Clients für gelegentliche Tests
 - über Cron-Job in Fileserver, bei „Sophos-versorgten Clients“ kann 2nd-Opinion-Scanner sinnvoller sein (z.B. ClamAV)

Mac-OS-X

- Einsatz ist wie bei Windows als verpflichtend anzusehen.
- Private Version von Sophos generell kostenfrei.

Mobile

- Keine Lizenz vorhanden, wäre komplette Mobile-Control-Suite.
- Bei Universitäts-Geräten fehlt hier etwas, kostenlose Antiviren anderer Hersteller für privat verfügbar

EOL

Windows-9x, -NT, Mac-OS-Classic, alte Mac-OS-X-Versionen, Novell

Problembeschreibung

- Sophos hat Signatur ausgeliefert, die das Auto-Update von Sophos als Malware erkennt.
- Betroffen sind Windows-PCs, die am 19.9. gegen 22 Uhr an waren.
- Betroffen sind auch viele Auto-Updater anderer Programme.
- Sophos-Update keine Lösung, da Auto-Updater blockiert ist. Sophos-Live-Schutz würde helfen.

Auswirkung LUH: *vielen* betroffene Clients

private PCs („home“) völlig unklar, LUH-PCs dank ausgebautem Reporting eher

Aufräumen

- viele PCs ließen sich über Policy-Änderungen nach-und-nach reparieren, (allerdings nur EM-verwaltete, Policy über CID nicht)
- Rest ist nur als Admin am Client selbst reparierbar
- noch immer über 200 unique-IPs in SNMP-Logs, wir schreiben Institutsadmins mit IP-Listen an
- Details und Reparatur-Tool vgl.
http://www.rrzn.uni-hannover.de/sophos_shhupdaterb.html
- Updates anderer Programme:
 - nach Reparatur Updates anstoßen & durchführen
 - bei Policy „Malware sofort löschen“ ... neu installieren!

Lehren

- gemanagte Clients leichter reparierbar
 - Reporting ist sehr hilfreich,
Aufwand der Einführung hat sich gelohnt.
 - Policy, Malware automatisch zu löschen, ist schlecht!
 - False-Positive können immer vorkommen, evt. später korrigiert.
 - Daten-Dateien können betroffen sein, denen Daten noch immer sicher entlockbar sind.
 - Dateien können einer Person gehören, rechtlich bedenklich.
- Verschieben ist okay, einfach nur Blockieren ist zu empfehlen.

2 kritische Veröffentlichungen (Tavis Ormandy):

- 1 Sophail: A Critical Analysis of Sophos Antivirus
- 2 Sophail: Applied attacks against Sophos Antivirus
 - Hauptkritik: zögerliche Reparatur durch Sophos
 - angesprochene Sicherheitslücken größtenteils geschlossen
 - „Lieblosigkeiten“ des Clients auch an anderen Stellen sichtbar:
 - SNMP-Traps: lokalisiert, wenig strukturiert
 - private oder Link-Local-IPs im Reporting

aber:

- unklar, wie AV-Produkte anderer Hersteller dastünden
- ohne Anti-Virus ist keine Alternative:
Risiken ohne deutlich größer als mit.

Anmerkungen:

- Windows-Computer-Name soll zukünftig Subdomain enthalten:
DNS `host.instkuerzel.uni-hannover.de`
`pc220hh.rrzn.uni-hannover.de`
Win `left(left(instkuerzel,6)+'_'+host,15)`
`rrzn-pc220hh` (in der Domäne: `rrzn-pc220hh.rrzn.intern`)
nötig für zentrales Management, Bekanntmachung wird folgen.
- Policies für gemanagte Clients je Einrichtung anpassbar, jedoch nicht zu kleinteilig, eher statisch

Fragen:

- Live-Schutz und Web-Schutz generell aktivieren?
- Bedarf an AV-Schutz über Linux-Fileserver?
- Bedarf an Mobile-Control-Suite, ggf. welche Architektur?