SOPHOS (unter Linux)

Sicherheitstage SS 2006

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

16.06.2006

SAV für Linux:

- 4.0
- 5.x

Sophos SAV:

- 6.0 für Windows
- Ankündigungen

Überblick

- erkennt Viren etc., die für Windows oder MacOS sind
- nur x86-Plattform (64-Bit ab Version 5)

Einsatzszenarien

- File-Server (Samba)
- Mail-Storage
- Web-Server, der Binaries/MS-Office-Dateien/PDFs bereitstellt
- Scanning von Medien:
  - USB-Stick (z.B. vor Versendung per Mail)
  - Scanning vor dem CD-Brennen nach Software-Download
  - Windows-Partition aus sauberem System (z.B. Boot-CD)

R|R|Z|N

Funktionen

Sweep

- Erkennung von Windows- & MacOS-Malware
- nur Kommandozeilen-Tool,
  Aufruf z.B. als `cron`-Job
- Auto-Update (Signaturen & Engine)

Intercheck

- ermöglicht zentrale Auswertung von verschiedenen Hosts
- müsste manuell konfiguriert werden
- Verwendung unnötig, insb. mit SAV >4.0 zweifelhaft

Installation

uh-sau

Wie bisheriges `sau.exe`, nur für Linux:

- `uh-saulin.tar.gz`-Datei
- `uh-saulin_*.deb`-Datei für Debian/Ubuntu-Systeme
- `.rpm`-Datei: nehmen wir gerne auf ...

manuell

- Sophospaket `linux.intel.libc6.glibc.2.2.tar.Z` installieren
  - entpacken mit `uncompress`, meist auch `gunzip`; `tar`
  - ausführen von `sav-install/install.sh`
- Erstellen von `/etc/eminstall.conf`,
  Dokumentation in `sav-intsall/eminstall.txt`

Pfade in UH-SAU-Paket

- `/usr/local/bin|lib|man`: wie üblich
- `/var/local/cache/Sophos`: SAU-Downloadbereich
- `/var/local/lib/Sophos`: Engine, Signaturen
- `/etc/eminstall.conf`: SAU-Konfiguration

Debian-Paket

- nicht standardkonform (z.B. `/usr/local/`-Pfade)
- legt Cron-Job für Auto-Update an
- Auto-Update/Vollinstallation direkt nach Paketinstallation
- Installation mit `dpkg -i uh-saulin_*.deb`

- läuft als User `root` (schwer änderbar)

R|R|Z|N

neue Funktionen etc.

- on-access-scanning
- Web-Interface
- Standardsupport für Redhat, Suse, Turbolinux,
  aber auch sonst einsetzbar (z.B. problemlos unter Debian)
- Integration in Enterprise-Manager/Enterprise-Console

on-access-scanning

- benötigt Kernel-Module
  - „binary packs for supported kernels“ (gewisse Distributionen)
  - vom Installer compilierte für andere Kernels, Kernel-Sourcen und gcc müssen installiert sein ⟵aus Doku
- „talpa“-Technik (passt sich automatisch evt. ohne Neukompilierung an neue Kernels an) ⟵Supportauskunft
- optionale Komponente (ohne heißt keine Kernel-Abhängigkeit) installierbar sein.

Obige Aussagen scheinen widersprüchlich, bisher unklar. Tests auf System ohne gcc/Kernel-Sourcen stehen aus . . .

Auf Debian-System mit Kernel-Updates (Kernel-Sourcen: nein; gcc: ja) bisher keine Probleme, automatische Anpassung ist erfolgt.

User-Interface

Commandline

- Scannen mit `savscan`
- manuelles Update mit `/opt/sophos-av/bin/savupdate`
- unklar: Konfiguration auch ohne Web-GUI?

Web-Interface

- optionale Komponente
- lokaler Webserver (normalerweise Port 8081), Authentifizierung nötig
- dient eigentlich nur der Konfiguration & Log-Ansicht

- standardmäßig saubere Installation nach `/opt/sophos-av`, symbolische Links für Commandline-Tools nach `/usr/local/*`
- wohl gewisse Rechtetrennung (neben `root` auch `sophosav`)
- teilweise python-basiert, Python 2.4 nötig (zumindest wohl fürs Web-Frontend)

RRZN ist noch in der Testphase.

neue Funktionen

- Support für 64-Bit
- zunehmend Signaturen für Virenfamilien („GenoType“)
- Informationen zum Scannen gepackter Viren nicht in Engine sondern in Signatur-Dateien
- Removal (z.B. auch von Registry-Einträgen; für zunächst neue/wichtige Viren)
- Erkennung von Adware, Dialern
- Verbot bzw. nötige Genehmigung gewisser fragwürdiger Applikationen

- Personal-Firewall (Lizenznahme durch UH/RRZN noch unklar)

Umstellung Windows-Clients

Sophos Support

- derzeit für 4.0 nur noch Signatur-Updates
- Support für 4.0 endet 02/2007

RRZN & UH

- Engine-Download endet 07/2006
- Support endet 11/2006
- Neuinstallationen demnächst mit 6.0 möglich,
  nach Testphase zwingend für Neuinstallationen
- automatische Client-Umstellung von 5 auf 6 per Auto-Update

Web-Adressen / Tests

Direkt-Download

Die Programmpakete sind innerhalb der Universität auch ohne Webbrowser aus dem Sophos-Downloadbereich direkt downloadbar (für automatische Installationen etc.), z.B.

`http://www.rrzn.uni-hannover.de/fileadmin/SOPHOS/uh-sauxp.exe`

Zugriffstest für SAU

Funktioniert das Auto-Update nicht, testen Sie zunächst die Verbindung mittels Webbrowser für

`http://sophosupd1.rrzn.uni-hannover.de/Sophos/`

okay lokales Problem mit Sophos oder Personal-Firewall

Fehler Netzwerkverbindung, Personal-Firewall, RRZN-Server ?

Sophos

- Support für NT 4.0 nur noch bis Ende 2008
- langfristig Support für Legacy-Netware derzeit unklar
- Support für Windows-Mobile (PDA, Phones)
- verhaltensbasierte Rootkiterkennung, Rootkitentfernung

RRZN

- demnächst Knoppicillin in UH-Variante mit Sophos
- evt. vorkonfigurierte, tagesaktuelle Offsite-Installer
- evt. Übergang von MailMonitor auf Puremessage (bei Institutsinstallationen)