

samba-vscan

Vortrag für den LinuxTag 2005

Rainer Link

rainer@openantivirus.org

www.openantivirus.org

Agenda

- Einführung
- Features
- Installation
- Demo
- Ausblick
- Fragen/Feedback et al

Einführung

- Ermöglicht Virenüberprüfung beim Zugriff
- Unterstützt Samba 2.2.x und 3.0.x
- Als AV-Programme werden unterstützt u.a.
 - H+BEDV AntiVir
 - ClamAV / ScannerDaemon
 - FRISK F-Prot
 - F-Secure AV
 - Kaspersky AV
 - Sophos Sweep
 - Trend Micro

Features

- Überprüfung beim Öffnen/Schließen
- Bei Infektion wird Zugriff verweigert
- Quarantäne oder Löschen möglich
- Benachrichtigung an Anwender via Windows Message Service (winpopup)
- Logging via syslog
- Dateien können über Dateigröße und -typ von Prüfung ausgeschlossen werden
- internes Caching von Scan-Ergebnissen

Installation (I)

- Zur Kompilierung werden die Samba-Sourcen benötigt
- Samba: „./configure && make proto“ notwendig
- samba-vscan:
 - ./configure –with-samba-source=</path/to/source>
 - make
- Kopieren der Module und Konfigurationsdatei ggf. von Hand

Installation (II)

- Anpassen von smb.conf, z.B.
[homes]
vfs objects = vscan-clamav
vscan-clamav: config-file =
/etc/samba/vscan-clamav.conf
- Reload von Samba (killall -HUP smbd)

Demo ...

Ausblick

- Samba4 Unterstützung
- Ausschluss über Dateinamen (regulärer Ausdruck)
- Samba 2.2.x Support wird entfernt (vereinfacht Code)
- Bugfixes ;-)

?!?

- Fragen
- Wünsche
- Vorschläge