AMaViS − A Mail Virus Scanner

Inhaltsverzeichnis

Autor: Rainer Link

E−Mail:RainerLink@gmx.de

Homepage:http://rainer.w3.to/

Weitere Informationen:
AMaViS − http://www.aachalon.de/AMaViS/

Beste Darstellung mit


AMaViS – A Mail Virus Scanner

http://www.aachalon.de/AMaViS/
amavis@aachalon.de
amavis−dev@aachalon.de

Referent

Rainer Link

- Mitglied in der Virus Help Munich seit November 1995
- Mitglied in der AmaViS−Entwicklergruppe seit Oktober 1999
- eMail: RainerLink@gmx.de
- Web: http://rainer.w3.to/

Virenschutz & Linux (Unix)

- Heterogene Umgebung (Linux, FreeBSD etc. als Server & Windows–Clients)
- ICSA–Studie: Virenverbreitung v.a. via eMail–Attchments (Makro–Viren!)
- kombinierter Client–/Server–Virenschutz ist »state–of–the–art«
- AMaViS fängt infizierte Attachments direkt am eMail–Gateway ab

Systemvoraussetzungen

- Ein oder mehrere Virenscanner (McAfee VirusScan, H+BEDV AntiVir/X, KasperskyLab AVP, Sophos AntiVirus)
- installierter & funktionierender MTA (sendmail oder qmail)
- metamail
- Entpacker (u.a. uudecode, gunzip, unzip)

Installation (1)

- Archiv entpacken
- Doku lesen :–)
- ./configure
- make
- make install
- sendmail.cf anpassen

Installation (2)

- Anpassung sendmail.cf

  #Mlocal, P=/usr/bin/procmail, F=lsDFMAw5:/|@SPfhn,
  S=10/30, R=20/40,
  # T=DNS/RFC822/X−Unix,
  # A=procmail −Y −a $h −d $u

  Mlocal, P=/usr/sbin/scanmails, F=lsDFMAw5:/|@SPfhn,
  S=10/30, R=20/40,
  T=DNS/RFC822/X−Unix,
  A=scanmails −Y −a $h −d $u

- killall −HUP sendmail

Verfügbare Patches

- rl–patch2a
- outmail–patch (»add–on«)
- rl–smtp–patch1

rl–patch2a – Übersicht

- Bugfix beim Aufruf von AVP
- Erweitert AMaViS um DataFellows F–Secure AV und KasperskyLab AvpDaemon (–Client)
- Erleichtert Änderungen der Warn–eMails an Absender und Empfänger

rl–patch2a –Installation

- Archiv ins AMaViS–Verzeichnis entpacken
- ./amavis–patch.sh
- ./configure
- make
- ggf scanmails.sender o. scanmails.adressee anpassen
- make install

rl–smtp–patch1

- zur Überprüfung auch von ausgehenden eMails
- benötigt smtpd/smtpfwdd aus dem Juniper Firewall Toolkit (von Obtuse)
- benötigt rl–patch2a
- »proof–of–concept«

rl–smtp–patch1 – Installation (1)

- Juniper Toolkit entpacken
- Makefile für smtpd/smtpfwdd anpassen
- make und make install
- rl–smtp–patch1 ins AMaViS Source–Verzeichnis entpacken
- ./amavis–smtp–patch.sh
- ./configure, make und make install
- Änderungen in sendmail.cf rückgängig machen

rl–smtp–patch – Installation (2)

- Start–Script für smtpd/smtpfwdd schreiben oder inetd.conf anpassen
- sendmail läuft nicht mehr in Daemon, sondern wird per cron–job aufgerufen (z.B. alle 10min)

Nachteile/Probleme

- Riesiges »Script–Monster« (Verstoß gegen KISS–Prinzip)
- Aufruf zahlreicher (externer) Programme (grep, sed, metamail & Co)
- »blindes« Vertrauen auf Rückgabewerte und Environment–Variablen
- Performance
- manuelle Konfiguration

Zukunft (?!)

- Rewrite in Perl (?)
- einfachere & automatische Installation sowie Konfiguration
- (bessere) Unterstützung diverser MTAs
- www.amavis.org – PHP3 mit MySQL
- ...

(kommerzielle) Alternativen

- Trend Micro InterScan VirusWall
- H+B EDV AvGuard
- ???

URLs

- http://www.aachalon.de/AMaViS/
- http://av−linux.w3.to/
- http://www.antivirus.com/
- ftp://ftp.antivir.de/

Legal Stuff

- AMaViS unterliegt der GNU General Public License
- diese Präsentation unterliegt der OpenContent License