Antivirus sur serveur de messagerie Unix

- Problématique
- Principe
- Solution
- Installation

Antivirus centralisé
Problématique

- Premier ver apparu en novembre 1988
- Accroissement très important des incidents viraux depuis 1990
- Coût estimé des vers et virus sur plate formes Microsoft Outlook en 2001 : 8000 milliards de dollars US
- Principaux problèmes:
  - Attaques vers des serveurs de messagerie (MTA: Mail Transport Agent ex sendmail): Mail bombing, buffer overflow
  - Attaques vers des clients de messageries (MUA: Mail User Agent ex elm, pine, mail, mailx): virus, macrovirus, vers
  - Attaques de désinformation: hoaxes, spam, usurpation d'identité

Antivirus centralisé
Stratégies

- Approche locale : Poste client
- Approche globale : Poste serveur

Ces deux solutions sont complémentaires et doivent faire appel à des moteurs antiviraux de fournisseurs différents

Antivirus centralisé

- Approche antivirale locale:
  - **Problème**: Mise à jour de la table de définitions de virus sur chaque poste client
  - **Solution automatique**: on retrouve les problèmes liés à la distribution de logiciels (live update, etc.)
  - **Solution manuelle**: envoi d'un mail à tous les utilisateurs leur demandant de récupérer la mise à jour sur un serveur interne
- Avantages: Intégration des utilisateurs à la politique sécurité
- Inconvénients: La mise à jour risque d'être effectuée après l'arrivée du virus sur le poste client.

Antivirus centralisé

- Approche antivirale globale :
  - Interception des messages entrant sur le serveur de messagerie avant d'atteindre les postes clients.
- **Avantages** : Mise à jour de l'antivirus sur une seule machine, le serveur de messagerie.
- **Inconvénients** : Charge système générée , délai de réponse.

Solution intéressante dans un environnement de clients hétérogènes Unix, Windows, Macintosh utilisant des clients pop, imap, etc.

Antivirus centralisé

- MUA, MTA, LDA : Définitions
  - **MUA** (Mail User Agent) : Programme exécuté par un utilisateur pour le traitement des messages (Elm, pine, Netscape Messenger, Microsoft Outlook, Qualcomm, Eudora, etc.)
  - **MTA** (Mail Transport Agent) : Programme exécuté par un serveur de messagerie pour envoyer et recevoir des messages (écoute sur le port smtp et fourniture du service smtp port 25) (Sendmail, postfix, exim, qmail, courier, smail; etc.)

Antivirus centralisé

- **LDA** (Local Delivery Agent) : Programme utilisé par un serveur de messagerie pour délivrer les messages dans les boites aux lettres des utilisateurs: « Local Mailer »
(Procmail, maildrop, deliver, mail, tmail, dmail, etc.)

Sendmail est utilisé comme MTA et LDA. Ces deux fonctions sont implémentées dans le même programme.

- On peut cependant utilisé un LDA différent si on le souhaite par un .forward :

" |IFS=' '&&exec /usr/local/bin/procmail –f- || exit 75 "

Antivirus centralisé

- Intégration de 3 parties logicielles:

1) MTA
2) Scanner de virus
3) Antivirus

Antivirus centralisé

Fonctionnement

- Le scanner de virus tourne au niveau du LDA

Quand un mail arrive sur le serveur de messagerie:

- Extraction et décompactage si nécessaire des documents attachés , puis scan par un antivirus
- Exemples de scanners de mails freeware
  - Amavis
  - Mailscanner
  - Procmail/Sanitizer

Antivirus centralisé Mailscanner

- Version 3.15-3 du 20 mai 2002
- Plate formes Solaris, Linux, BSD, AIX, HP-UX
- http://www.sng.ecs.soton.ac.uk/mail scanner
- Sous licence GPL (GNU Général Public Licence)
- Supporte sendmail et Exim comme MTA (ni Postfix ni Qmail aujourd'hui)
- Peut être associé à 8 antivirus commerciaux:
  - Sophos, Uvscan mais aussi F-Prot, F-Secure, Kapersky, CommandAV, InoculateIT
- Langage de programmation PERL et Shell Unix

Antivirus centralisé Mailscanner

- Détection possible de spams
- Ajout de signature sur les messages scannés
- Remplacement des fichiers attachés infectés par un message personnalisable expliquant ce qu'il est advenu
- Les fichiers attachés contenant des virus sont automatiquement désinfectés et envoyés au destinataire
- Notification au postmaster de virus trouvés ainsi qu'à l'émetteur (quand l'adresse d'émission est une adresse réelle)
- Arrêt des messages émis en local si infection.

Antivirus centralisé
Mailscanner (Principe)

- Mailscanner
  1) collecte les messages de la queue entrante
  2) Teste les messages pour voir si ce sont des spams
  3) Déplace les messages en texte basique ascii vers la queue sortante et les délivre à leurs destinataires
  4) Décompacte les fichiers MIME des messages restants
  5) Lance un scan antiviral
  6) Scanne les extensions de fichiers non standards (ex : txt.bvs)
  7) Déplace les fichiers infectés vers une zone de quarantaine
  8) Remplace les attachements infectés par un texte explicatif

Antivirus centralisé
Mailscanner (Principe)

- Mailscanner
  1) Ajoute un message au message d'origine encourageant le destinataire à lire les attachements remplacés
  2) Déplace les messages sains vers la queue de sortie
  3) Reconstruit les messages modifiés dans la queue de sortie
  4) Efface les messages originaux de la queue entrante
  5) Assure la délivrance des messages présents dans la queue de sortie
  6) Avertit le postmaster local et les expéditeurs des infections trouvées
  7) Si possible, désinfecte les attachements d'origine et les envoie avec une note explicative

Antivirus centralisé Mailscanner et sendmail

- Sendmail fournit les services smtp et délivrance de messages dans le même process
- Il écoute sur le port 25, place les messages dans la queue et délivre les messages à leurs destinataires
- En utilisation avec mailscanner, on lance deux sendmails:
  - l'un en écoute sur les mails entrants qui place les messages sur une « incoming queue »
  - l'autre chargé de l'acheminement des mails après traitement par mailscanner

Antivirus centralisé Mailscanner et sendmail

- Mailscanner collecte les messages sur la queue d'entrée, les teste et les filtre, puis les place sur la queue de sortie .
- Le deuxième process sendmail se charge de l'acheminement.

Antivirus centralisé
Mailscanner Avantages

- Le découpage de sendmail en 2 process sendmail est extrêmement facile à réaliser:
  - pas de recompilation
  - Pas de changement du fichier de configuration sendmail.conf
  - Le premier sendmail agit comme MTA (écriture dans « incoming queue »
  - Le second sendmail agit comme LDA (lecture de « outgoing queue »

Antivirus centralisé
Mailscanner

- /etc/rc2.d/S88sendmail

```
Case "$1" in
'start')
      if  [-f /usr/lib/sendmail –a –f /etc/mail/sendmail.cf  ]; then
            if  [ ! –d /varmail/mqueue ]; then
                        /usr/bin/mkdir –m 0750 /varmail/mqueue
                        /usr/bin/chown root:bin /varmail/mqueue; then
             fi
            if  [ ! –d /varmail/mqueue.in]; then
                        /usr/bin/mkdir –m 0750 /varmail/mqueue.in
                        /usr/bin/chown root:bin /varmail/mqueue.in
             fi
       /usr/lib/sendmail –bd –ODeliveryMode=queueonly –
     OQueueDirectory=/varmail/mqueue.in
       /usr/lib/sendmail –q15m&
     fi
```

Antivirus centralisé Mailscanner

- **Crontab root :**

```
# Mise a jour quotidienne antivirale
13 0 * * * /opt/sophos/bin/autoupdate 2>&1 > /dev/null
#Teste le scanner anti-virus toutes les 20 minutes
0,20,40 * * * * /opt/mailscanner/bin/check_mailscanner 2>&1
> /dev/null
#
```

Mailscanner

From - Fri May 24 08:42:36 2002
Received: (from root@localhost)
by newb6.u-strasbg.fr (8.9.3/8.9.3) id BAA04498;
Fri, 24 May 2002 01:53:28 +0200 (MET DST)
Date: Fri, 24 May 2002 01:53:28 +0200 (MET DST)
From: "MailScanner" <postmaster@newb6.u-strasbg.fr>
To: postmaster@newb6.u-strasbg.fr
Subject: Warning: E-mail viruses detected
The following e-mail messages were found to have viruses in them:

Sender: <buatois@ismea.fr>
Recipient: <untel@newb6.u-strasbg.fr>
Subject: Japanese lass' sexy pictures
MessageID: BAA03701
Report: >>> Virus 'W32/Klez-G' found in file ./BAA03701/stat_tel
MailScanner
Email Virus Scanner