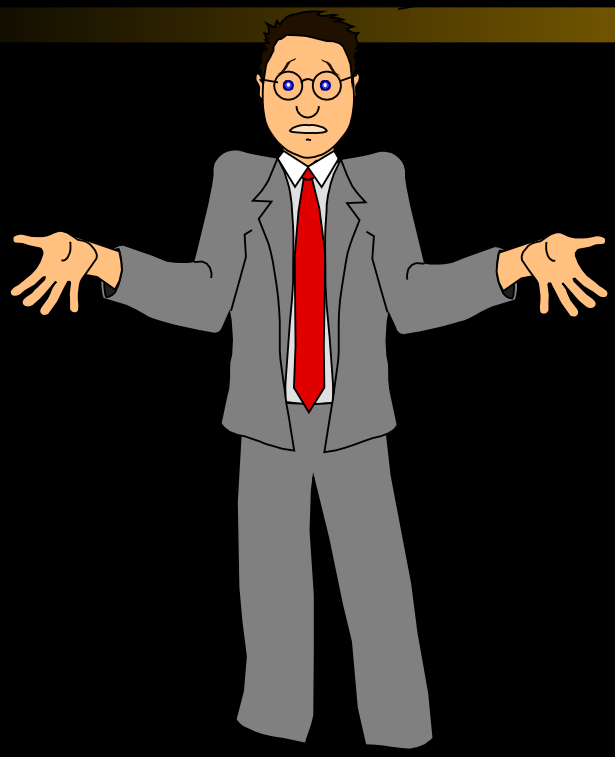
Antivirus per mailserver: RAV Antivirus & altri

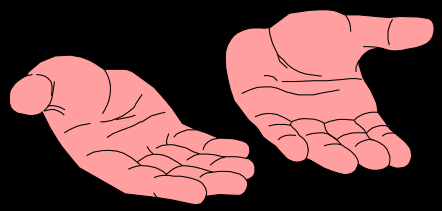
Marco De Rossi
I.N.F.N. Sezione di Roma
I.C.R. - Servizio Impianti Calcolo e R
mail: Marco.DeRossi@Roma1.infn

Introduzione



Perche` installare un AntiVirus sui mailserver di Sezione?

Introduzione



- Per cercare di limitare quanto piu’ possibile i danni causati dalle e-mail che contengono degli attachment “pericolosi”.

Introduzione

- OK. Dopo aver installato l'AntiVirus sul mailserver di Sezione potro' tranquillizzare tutti i miei utenti sul fatto che non riceveranno piu' nessuna e-mail "infetta" ?

Introduzione

- Assolutamente NO!

L'aggiornamento del database dei virus conosciuti richiede del tempo non indifferente, tempo all'interno del quale il nuovo "virus" puo' diffondersi e fare danni senza poter essere riconosciuto e fermato.

Panoramica sui vari Sw-AV

In seguito alle e-mail circolate sulla lista apm@garr.it verso la fine del 2001 abbiamo voluto provare alcuni dei software AntiVirus esistenti.

- Inflex + un qualsiasi Virus Scanner Software
- Amavis + un qualsiasi Virus Scanner Software
- RAV Antivirus

Inflex

E’ stato installato con successo insieme al seguente Virus Scanner: Sophos, ma si e’ subito evidenziato un problema che non si e’ riuscito a risolvere:

- Il mailserver di Sezione non era piu’ in grado di riscrivere il campo “From” nella sintassi Nome.Cognome@dominio: faceva uscire le e-mail come username@dominio!!!

Inflex

- Provando a contattare il supporto non si e' ottenuta nessuna risposta.
- E' stato pertanto ritenuto non essere un software affidabile.
- Link di riferimento:

  http://www.pldaniels.com/inflex/

Amavis

Tra i prerequisiti necessari alla sua installazione erano citati 11 moduli perl.

Visto che il kit di installazione non li includeva, si notava immediatamente che per avere un AntiVirus installato correttamente sul mailserver bisognava soddisfare troppe dipendenze:

Moduli Perl + Amavis + Virus Scanner, ed un aggiornamento ad uno qualsiasi di questi 3 software avrebbe potuto pregiudicare il buon funzionamento del tutto. Da notare anche che essendo sviluppati da 3 “entita’” differenti, in caso di problemi, ognuna avrebbe potuto passare la palla all’altra.

Amavis

- Anche in questo caso pertanto abbiamo abbandonato la strada di Amavis.

- Link di riferimento:

  http://www.amavis.org/

RAV Antivirus

- E’ stato installato con successo ed e’ un “pacchetto unico” che ha tutto il necessario nel proprio “kit” di installazione. Non e’ un “wrapper” che necessita di un AntiVirus e non e’ un AntiVirus che necessita di un “wrapper”, e’ entrambe le cose ☺.
- Il supporto tecnico e’ buono: inizialmente abbiamo incontrato delle difficolta’, ma sono state superate grazie alle risposte che ci hanno fornito.

RAV Antivirus

- E' disponibile per vari MTA (Sendmail, Qmail, Exim, ….) e per vari OS (Linux, FreeBSD, Solaris, Windows, …. NO Compaq ☺).

- E' disponibile sia per Desktop che per Mail Servers.

RAV Antivirus

- Noi abbiamo installato sul nostro mailserver la versione “ravmilter per sendmail per linux v8.3.2”.
- E’ stato installato su di un PC 2µP Pentium III 800Mhz 1GB RAM con RAID HW offerto dal Promise on-board, con Linux RH 7.1 Kernel 2.4.2-2, e con sendmail v8.11.6 compilato con l’opzione libmilter che dalla versione RH 7.2 c’e’ di default.

RAV Antivirus

- E’ configurabile a piacere: gli si puo’ dire di intraprendere varie azioni (reject, delete, clean, ignore, …) quando trova ad esempio attachment “infetti”, “sospetti”, quando trova all’interno del testo della e-mail, o del subject, parole “chiave” (porn, sex, …) ….

RAV Antivirus

- Auto-aggiorna il database della definizione dei virus conosciuti. Il default e': ogni ora, e finora sono sempre stati tempestivi nell'aggiornare il db per i nuovi virus.
- Sono attive delle discussion-lists su cui circolano informazioni utili e su cui il supporto tecnico offre anche soluzioni ai problemi (oltre a darne personalmente con indirizzi e-mail dedicati).

RAV Antivirus

- Il software “scansiona” solo le e-mail provenienti o dirette al dominio per il quale si e’ acquistata la licenza.

- Link di riferimento:

http://www.ravantivirus.com/

RAV Antivirus

Costi gia' scontati e senza IVA:

- Licenza base (per 2 domini di posta elettronica): 222,08 €

  L'aggiornamento per gli anni successivi costa: 69,50 €

- Licenza per 3 domini: 234,08 €

  L'aggiornamento per gli anni successivi costa: 73,50 €

Fine

Questo talk e` anche su Web
alla URL:

http://www.roma1.infn.it/sicr/seminari/talk-rav-labiodola-2002.html

altri riferimenti:
http://www.ts.infn.it/conferences/ccr2002/