Linux Day 2003

Davide Casale, Politecnico di Torino

Sicurezza :
una parola, mille pericoli.

29 Novembre 2003

Sicurezza : cos'è ?

E' la garanzia dei requisiti di:

- RISERVATEZZA
- INTEGRITA'
- DISPONIBILITA'

dei servizi elaborativi e dell'informazione.

Riservatezza :

Le informazioni riservate devono essere accessibili solo da parte di persone autorizzate

Integrità :

- Completezza (informazione completa)
- Accuratezza (informazione senza errori)
- Validità (informazione deriva da processi validi ed autorizzati)

Disponibilità :

L'informazione deve essere presente ed utilizzabile in un tempo adeguato alle necessità operative sia aziendali sia dei Clienti.

Sicurezza : perchè ?

- Caratteristica di qualità del software o del servizio
- Difesa attività e beni
- Difesa dell'immagine
- Adempimenti di Legge
- Motivazioni economiche

- **Sicurezza: cos'è?**
- **Sicurezza: perché?**
- **Sicurezza: come?**
- **HW/SW proprietari**
- **SW opensource**
- **Vantaggi opens.**
- **Svantaggi opens.**
- **Elementi base della sicurezza di rete**
- **Prodotti opensource per la sicurezza**

Tramite apparati
Informatici
(hardware)
in grado di svolgere
specifiche funzioni
di controllo attivo e
passivo
(software)

Il software utilizzato
per svolgere le funzioni
di controllo della sicurezza
informatica può essere

Proprietario

o

Open Source

HW/SW proprietari

Sviluppati da aziende ed utilizzati come scatole nere per svolgere la loro funzione specifica di sicurezza

SW opensource

Sviluppati da appassionati o gruppi sponsorizzati da aziende, ma con il rilascio pubblico del codice che esegue la funzione di sicurezza

Vantaggi opensource

- Disponibilità del codice
- Maggiore flessibilità potendo modificare internamente il codice
- Tempi rapidi per le patch di sicurezza

Svantaggi opensource

- Minor supporto diretto al prodotto
- Più complesso (o minor user friendly)
- Necessità di personale con maggior know-how

Elementi base della sicurezza di rete :

- Firewall
- Intrusion Detection (IDS)
- Antivirus
- AntiSpam
- Proxy Server
- Content Filtering

Firewall

La porta blindata della rete:

permette di controllare tutto quello che entra o esce dalla nostra rete locale e decidere cosa può passare e cosa no

Intrusion Detection (IDS)

La telecamera nascosta della rete:

ascolta tutto il traffico di rete in modalità passiva e genera allarmi a seconda di specifici eventi che accadono sul traffico di rete

AntiVirus

(per MailServer, di Flusso, sui client)

MailServer: controllo e-mail

Flusso: controllo navigazione (http, ftp)

Client: controllo file dell'utente sulla sua macchina

AntiSpam

Il software di AntiSpam solitamente si posiziona o su client o sul server di posta e 'cerca' di identificare la posta spazzatura e di scartarla a priori automaticamente

Proxy Server

Eroga due funzionalità :

- Caching per ottimizzare la banda di rete
- Log per controllare nel dettaglio la navigazione degli utenti

Content Filtering

Controllo a livello applicativo dell'uso della rete da parte dell'utente (parental control). Blocco di siti per categoria (porno, gioco di azzardo, etc.) o di e-mail per contenuto (spionaggio industriale, etc.)

Sicurezza: cos'è?

Sicurezza: perché?

Sicurezza: come?

HW/SW proprietari

SW opensource

Vantaggi opens.

Svantaggi opens.

Elementi base della sicurezza di rete

Prodotti opensource per la sicurezza

- Firewall : Linux IPTABLES
- IDS : SNORT
- Antivirus* : MailScanner
- AntiSpam : Mozilla e SpamAssassin
- Proxy Server : Squid
- Content Filtering : MailScanner e SquidGuard

- Sicurezza: cos'è?
- Sicurezza: perché?
- Sicurezza: come?
- HW/SW proprietari
- SW opensource
- Vantaggi opens.
- Svantaggi opens.
- Elementi base della sicurezza di rete
- **Prodotti opensource per la sicurezza**

Firewall : Linux IPTABLES

www.netfilter.org

Firewalling satefull inspection
del kernel di Linux
(dalla versione 2.4)

IDS : SNORT

www.snort.org

Intercetta tutto il traffico sul troncone di rete dove è posizionata la macchina sulla quale è installato e genera allarmi a seconda del contenuto del traffico di rete (signature)

Antivirus* : MailScanner

www.mailscanner.info

MailScanner si inserisce su server di posta open source come sendmail o postfix e controlla tutta la posta con un motore di antivirus commerciale (f-prot, sophos, mcafee, trend, etc.)

Antivirus* : MailScanner

Mantenere aggiornate le signature di un antivirus è un lavoro pesante. Non ci sono antivirus veri e propri open source.

Per ora...

AntiSpam : Mozilla e SpamAssassin

www.mozilla.org

www.spamassassin.org

Mozilla Client di Posta ha un ottimo AntiSpam adattativo

SpamAssassin sui server (ad esempio con MailScanner)

- Sicurezza: cos'è?
- Sicurezza: perché?
- Sicurezza: come?
- HW/SW proprietari
- SW opensource
- Vantaggi opens.
- Svantaggi opens.
- Elementi base della sicurezza di rete
- **Prodotti opensource per la sicurezza**

Proxy Server : Squid

www.squid-cache.org

In grado di svolgere diverse funzioni evolute oltre al caching e log (autenticazioni varie, ottimizzazione delle richieste dns, etc.)

Content Filtering : MailScanner e SquidGuard

MailScanner permette anche un controllo e filtraggio sul contenuto delle e-mail transitanti dal server di posta

SquidGuard permette di bloccare o permettere la navigazione su siti specifici o per keyword contenute nel sito chiamato

Domande finali