marco.filippi@dei.unipd.it

Gruppo di lavoro

Sicurezza di rete
“Firewall e IDS”

Padova
19 luglio 2007

Cos'è un firewall

"un firewall [omiss.] è un componente passivo di difesa perimetrale (hardware o software) che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.

[omiss.]

La sua funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti"

da http://it.wikipedia.org/

Cos'è un IDS

“L'Intrusion Detection System o IDS è un dispositivo software e hardware [omiss.] utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.
[omiss.]
Un IDS consiste quindi in un insieme di tecniche e metodologie realizzate ad-hoc per rilevare pacchetti sospetti”
da http://it.wikipedia.org/

Firewall e IDS sono complementari

ES. Web server

Il firewall impone che solo il server preposto sia raggiunto dalle richieste di pagine WEB

L'IDS analizza le richieste che transitano e controlla che non contengano anomalie ed eventualmente le segnala

Scopo del gruppo

- Aumento del livello di sicurezza complessivo della rete di ateneo attraverso il coordinamento delle strutture
- Standardizzazione delle procedure tecniche
- Sensibilizzazione al problema della sicurezza di rete

Attività svolte

- Individuazione dello stato dell'arte nelle diverse realtà
- Condivisione del know-how
- Collaborazione con l'Ufficio Legale

Obiettivi primari

- Individuazione di un insieme minimo di regole condivise
- Indicazioni tecniche per l'adozione di sistemi di firewalling
  - how to per la configurazione dei sistemi
  - creazione di una soluzione pronta all'uso basata su sw libero
- Strategie per la produzione, conservazione e utilizzo dei files di log

Obiettivi secondari

- Procedure tecniche per la gestione di incidenti informatici
- Condivisione tempestiva degli allarmi relativi ad incidenti informatici e delle relative soluzioni tecniche
- IDS - indicazioni sulla scelta e utilizzo

Necessità evidenziate

- Costante aggiornamento
  - tecnico
  - normativo

Risultati ottenuti

- Condivisione delle esigenze e delle esperienze riguardanti le problematiche di sicurezza della rete
- Consapevolezza della necessità di una gestione omogenea a beneficio della sicurezza complessiva della rete di Ateneo

Domande?