



Laboratorio di sicurezza dei protocolli di rete - lab_010

16 Febbraio 2007

**Master in progettazione e gestione di
sistemi di rete - III edizione**



Dipartimento di
Informatica



Agenda lab 010

LAB_010 Sicurezza dei Protocolli



Dipartimento di
Informatica

Agenda lab 010

- Gestione delle Patch
 - WSUS



Agenda lab 010

- ❑ Gestione delle Patch
 - ❑ WSUS

- ❑ Gestione di un Antivirus
 - ❑ Trendmicro



Window of exposure

The Window of Exposure is the period of time between the release of a new virus/exploit into the wild, and the point at which end-user networks are protected from that.



Rischi...

Le patch vengono pubblicate con una elevata frequenza.

La window of exposure tende ad aumentare.

Se aggiungiamo il tempo di applicazione delle patch...

Gestione delle patch

Una infrastruttura che conti molti client non può affidarsi ad una gestione manuale delle patch.

Esistono diversi prodotti quindi per automatizzare questo processo.

(es. WSUS, SMSserver, Landesk, etc)



Ambiente di test

Spesso le patch possono inibire qualche funzionalità delle applicazioni in uso.

I prodotti di *patch management* permettono di gestire un primo *deploy* su macchine di test, per poi passare ad un *massive deploy*.



Reboot

Un altro beneficio dei prodotti di patch management, oltre a permettere di non dover passare computer per computer, oltre a non interrompere il lavoro degli utenti, permette di utilizzare lo shutdown serale per l'applicazione delle correzioni.



Bandwidth

E' possibile inoltre scaricare dal produttore l'elenco delle patch, approvare quelle necessarie, scaricarle una volta soltanto e fare collegare i client sempre e solo al nostro server.



Statistiche

I prodotti di patch management permettono di avere il dettaglio delle patch da applicare, i computer da patchare, i computer aggiornati e così via.



- duplicare la macchina vmware windows
- rendere la prima domain controller
- installare e configurare WSUS
- configurare le policy
- fare il join al dominio della seconda VM
- approvare le patch
- verificare che le patch siano applicate



Antivirus

Tutte le considerazioni fatte in merito alla gestione centralizzata delle patch sono valide anche per il servizio di Antivirus.



Client

Nel caso di questo servizio è necessaria la possibilità di poter installare/aggiornare i client direttamente dalla console del server.



Disattivare il client

La gestione centralizzata impedisce all'utente di disattivare l'antivirus, ma lo permette all'amministratore sul singolo client a seguito di autenticazione sul servizio.



- ➔ installare sul DC la consolle antivirus
- ➔ installare il client da remoto
- ➔ verificare la protezione con eicar
- ➔ verificare le statistiche



Grazie!

Queste slide sono disponibili su

<http://www.scienze.univr.it/fol/main?ent=avvisoin&cs=105>

Per domande od approfondimenti:

alessio@alba.st



Dipartimento di
Informatica

These slides written by
Alessio L.R. Pennasilico
aka mayhem. They are
subjected to Creative
Commons Attribution-
ShareAlike 2.5 version;
you can copy, modify,
sell. "Please" cite your
source and use the same
licence :)