ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Firenze

INFNTC-06/13
17 Ottobre 2006

STRATEGIE PER L'UPDATE MANAGEMENT PROCESS

Francesca Del Corso

INFN, Sezione di Firenze

Abstract

L'articolo si propone di illustrare le metodologie per il sofware update ed il Security Patch Management su piattaforma Microsoft mostrando quali sono i processi, i tool e le utility per tenere aggiornati i propri sistemi minimizzando l'occorrenza e la gravità di possibili attacchi che sfruttino le vulnerabilità presenti sui sistemi.
Il documento contiene inoltre una panoramica dei test effettuati presso la sezione INFN di Firenze e sull'attuale ambiente di produzione, proponendosi come linea guida e di consultazione per le altre sezioni INFN.

PACS: 89.70.+c

*Published by **SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

Introduzione

L'*Update Management Process* è un processo che coinvolge tutte le piattaforme: i maggior produttori di software (Microsoft, Cisco, Sun, RedHat, FreeBSD) rilasciano continuamente patch di sicurezza relative a identificate vulnerabilità dei propri sistemi.
L'importanza del processo si evidenzia in presenza di attacchi: infatti è in questo momento che si possono verificare i downtime dei sistemi, che hanno come conseguenza:
a. interruzioni di sistemi critici, perdita o danneggiamento di transazioni critiche, perdita di produttività da parte dell'utente finale;
b. costi per la risoluzione dei problemi causati (*remediation time*) e per il recupero e la messa in linea dell'ultimo backup;
c. perdita dei dati o danneggiamento degli stessi (*data integrity*);
d. possibilità di accesso a dati confidenziali e classificati, con eventuale perdita della proprietà intellettuale;
e. costi per l'attività legale di difesa e di investigazione dopo aver subito un attacco.
Una volta che il sistema è stato violato, l'applicazione delle patch di sicurezza non è più sufficiente, dunque una loro gestione proattiva è un requisito fondamentale per tenere le proprie reti e tecnologie sicure.

L’Update Management Process

Prima di iniziare il processo di aggiornamento dei sistemi (Fig. 1) devono essere eseguite una serie di operazioni:

- sottoscrizione ai *security alert* e ai servizi di informazione; è bene che gli amministratori di rete si registrino a ricevere notifiche via e-mail quando vengono pubblicati nuovi aggiornamenti critici in modo da essere tempestivamente informati sul rilascio di nuovi aggiornamenti per procedere rapidamente al test e alla distribuzione delle patch.
  Il *Microsoft Security Response Center* rilascia i propri bollettini di sicurezza mediamente una volta al mese, eccetto nei casi di exploit, nel qual caso la notifica avviene nelle 24 successive al rilascio della patch. Il *Security Bulletin Notification Service* notifica via e-mail il *Product Security Notification*, un alert tecnico e dettagliato, ed il *Microsoft Security Update*, un alert più generico, suddiviso per argomenti. Inoltre viene messo a disposizione il *Security Bulletin Web search tool* per la ricerca di informazioni su tutte le patch di sicurezza rilasciate, organizzato per prodotti e livelli. Diffidare da qualunque messaggio di posta elettronica proveniente da Microsoft contenenti file in attachment: la Microsoft non distribuisce mai software via e-mail.
- configurare gli strumenti di distribuzione automatica degli aggiornamenti
- definire una politica di sicurezza che preveda un piano di difesa e di risposta ad un attacco (*Emergency Security Response phase*): vanno stabilite le azioni da eseguire post incidente, in cui sono previste: 1) come valutare l’attacco; 2) individuare chi dovrebbe essere avvisato; 3) stabilire come isolare e contenere un attacco; 4) definire le azioni da eseguire per analizzare e rispondere ad un attacco; 5) definire cosa fare dopo avere subito un attacco. 6) definire strategie di *escalation* del problema.
- definire il o i responsabili del processo, ossia coloro che attuino il piano descritto al punto 2.
- preparare tutto il personale.

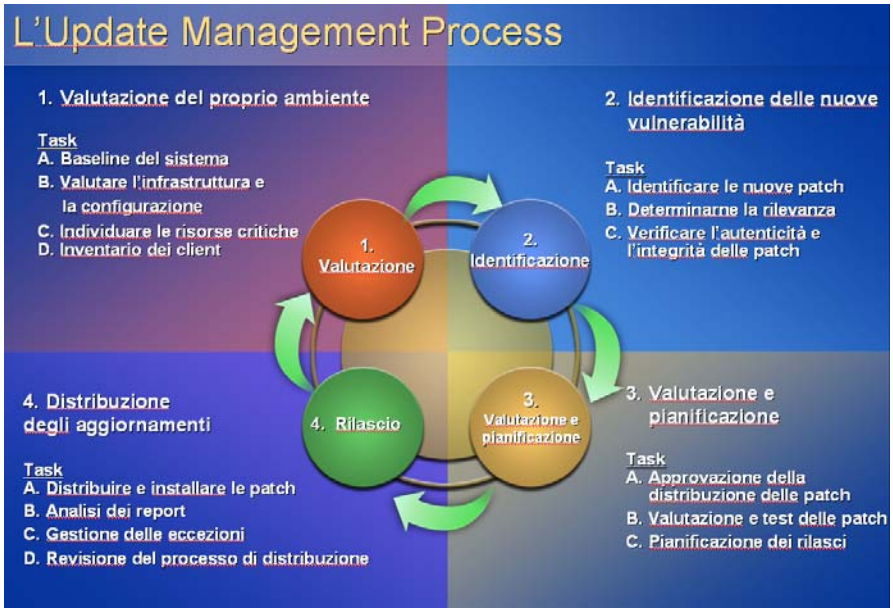

Fig. 1 – L'Update Management Process

Valutazione

La prima fase del processo di aggiornamento consiste nella valutazione del proprio ambiente di lavoro, ossia si deve:

1. conoscere quanti computer, prodotti e tecnologie sono presenti nel proprio ambiente;
2. sapere se esistono computer gestiti centralmente, ad esempio tramite un dominio;
3. quali sistemi operativi e quali versioni (italiano, inglese), quali applicazioni software e versioni vengono utilizzate nella propria LAN;
4. individuare le risorse critiche che si vuole proteggere (*asset*); queste informazioni verranno usate nelle fasi successive per impostare la priorità degli update e dei test che coinvolgono queste macchine;
5. eseguire un inventario del parco macchine presente nella propria sezione tramite strumenti di scansione in modo da arrivare a definire lo stato corrente dell'installato e degli applicativi usati
6. eseguire il *baseline* del sistema, ossia il processo di standardizzazione del parco macchine: a partire dall'inventario hardware e software vengono definiti gli standard a cui tutti i computer della rete devono aderire.
7. verificare quali computer rispettano il *baseline* e, per quelli che non lo rispettano, pianificare il loro allineamento, eseguirlo e controllarne i risultati ottenuti;

Identificazione

Questa fase prevede l'identificazione delle nuove patch attraverso la consultazione dei bollettini di sicurezza o dei web site appositi.
La terminologia con cui vengono indicate i vari tipi di security patch e di aggiornamenti software sono mostrate in Tab. 1.
Quindi prevede l'identificazione dello stato di vulnerabilità nei propri sistemi attraverso l'uso di strumenti per la scansione, IDS e virus detection, tenendo conto della rilevanza nel proprio ambiente dell'eventuale bug.
Viene quindi verificata l'autenticità e l'integrità delle patch, nonché la risposta appropriata alla vulnerabilità. Questo include il tipo di azione che è meglio eseguire; un software update oppure l'applicare contromisure che mitighino la vulnerabilità; quali cambiamenti sono richiesti; priorizzazione e schedulazione della release; chi è autorizzato ad eseguire l'approvazione.
Talvolta è meglio prendere contromisure piuttosto che installare un aggiornamento, poiché non può essere tollerato un downtime della macchina prolungato (ad esempio dovuto ad un riavvio), oppure sono meno rischiose da implementare, si applicano più velocemente, si eliminano più rapidamente (alcuni aggiornamenti non possiedono la possibilità di essere disinstallati). Generalmente le contromisure sono migliori quando è richiesta una risposta veloce ad una vulnerabilità.
E' fondamentale sapere in cosa consiste il cambiamento, su quali servizi va ad impattare, se la patch è in fase di sviluppo. Tipicamente le patch vengono applicate (e schedulate) in base alla loro criticità sui sistemi (Tab. 2).

TERMINE	DEFINIZIONE
Security patch	Un fix rilasciato per uno specifico prodotto che riguarda una vulnerabilità di sicurezza. Le viene assegnato un valore di criticità.
Critical Update	Fix rilasciato per uno specifico problema non relativo alla sicurezza.
Update	Fix per uno specifico problema non legato alla sicurezza e non critico.
Hotfix	Pacchetto composto da uno o più file che fissano un determinato problema, rilasciato dietro consenso di Microsoft. Sinonimi: QFE (*Quick Fix Engineering*), patch, update
Update rollup	Insieme di security patch, critical update, update e hotfix rilasciati insieme per un singolo prodotto (IIS, IExplorer)
Service Pack	Insieme di hotfix, security patch, critical update e update cumulativi emessi dall'ultimo rilascio del prodotto
Integrated Service Pack	Un prodotto e un service pack inclusi in un unico package
Feature pack	Nuove features per una release esistente, tipicamente inclusa nella succesiva

Tab. 1 Terminologia Microsoft utilizzata per gli aggiornamenti software

Priorità	Livello di severità MSRC della vulnerabilità	Definizione	Tempo raccomandato
1	Critical	Una vulnerabilità il cui exploit potrebbe far propagare un wirus/worm di Internet senza azione da parte dell'utente.	Nelle 24 ore
2	Important	Una vulnerabilità il cui exploit potrebbe compromettere l'integrità e la disponibilità di dati di utente e risorse/servizi (DoS)	Entro 1 mese
3	Moderate	Vulnerabilità del sistema mitigata da configurazioni di default, dall'auditing o difficoltà di exploit.	Nuovo S.P. o update rollup che include un fix entro 4 mesi
4	Low	Una vulnerabilità il cui exploit è difficile che si presenti oppure che ha un impatto minimo.	Nuovo S.P. o update rollup che include un fix entro 1 anno

Tab. 2 – Priorità e livello di severità delle patch

Valutazione e pianificazione

Questa fase prevede la preparazione di un'area di quarantena: tutti gli update software vengono scaricati, valutati e testati in un ambiente separato da quello di produzione, per verificarne l'impatto e valutare le eventuali compromissioni di applicativi e criticità presenti negli ambienti.
Viene inoltre determinata la loro approvazione per la distribuzione e la pianificazione dei rilasci.

Rilascio

Si tratta della fase di distribuzione degli aggiornamenti in cui avvengono la distribuzione e l'installazione delle patch, l'analisi dei report prodotti, la gestione delle eccezioni (errori, aggiornamenti mancanti), la revisione del processo di distribuzione o della politica di sicurezza: in risposta ad una vulnerabilità scoperta nel proprio ambiente può essere necessario rivedere la propria politica di sicurezza (*Enforce Security Policy*).

Strumenti per l'Update Management Process

Vediamo in dettaglio quali sono al momento le tecnologie e gli strumenti per l'aggiornamento dei nostri sistemi informatici, in relazione ai diversi scenari e dimensioni di una data sezione.

Tipo di utenza	Scenario	Scelta
Utente casalingo		Microsoft/Office Update
Sezione medio - piccola	Nessun server Windows	Microsoft/Office Update
	da 1 a 3 server, 1-3 amministratori di sistema	MBSA, WSUS
Sezione grande	Soluzione di patch management con livello base di controllo che aggiorna le ultime versioni del s.o.	WSUS
	Singola soluzione di Patch Management con elevato grado di controllo su aggiornamenti e distribuzione del sw	SMS

Tab. 3 – Soluzioni di Update Management.

Microsoft / Windows Update

E' lo strumento ideale per utenti individuali e Sezioni di piccole dimensioni.
Supportato da Windows 98, ME, 2000, XP, Windows Server 2003, questo tool permette di mantenere il computer aggiornato offrendo gli ultimi aggiornamenti al sistema di protezione, driver di periferica e altre funzionalità disponibili per il computer Windows.
L'utente seleziona l'icona *Start\Programs\Windows Update* oppure digita da command prompt *%systemfolder%system32\wupdmgr.exe* ed e' indirizzato al sito Internet http://windossupdate.microsoft.com da cui è possibile verificare se sono necessari aggiornamenti per Windows, l'hardware o le periferiche selezionando *Scan for updates* (Fig. 2).

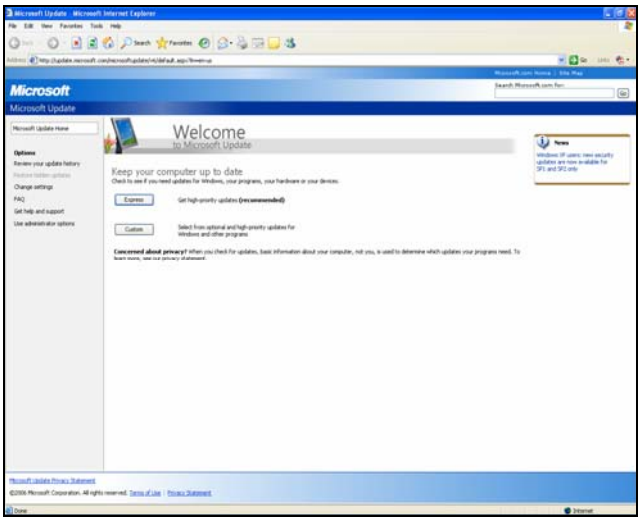

Fig. 2 – Microsoft Update.

Il codice client-side nel browser valida il server MU e scarica il catalogo dei metadata; questo codice utilizza i metadata per identificare gli aggiornamenti mancanti. L'utente seleziona gli aggiornamenti mancanti, quindi il client scarica, valida ed installa gli aggiornamenti, e successivamente aggiorna la history.
Per il singolo client è necessario un collegamento ad Internet e possedere i permessi di amministratore per poter installare le patch sul computer.
Nei sistemi da Windows 95 , 98, 2000 fino al SP1, il *Windows Critical Update Notification* (CUN) è un processo che gira in background mentre si è connessi ad Internet. Viene controllato il sistema ed indica se esistono nuovi update critici da scaricare. La connessione ad Internet è verificata ogni 5 minuti; se la connessione non viene trovata dopo la prima ora di ricerca, viene controllato se esiste una connessione in rete una volta ogni 60 minuti.
L'*Automatic Update* (AU), introdotta in Windows ME, rimpiazza il CUN ed è incluso in Microsoft Windows XP (Home e Professional), mentre viene aggiunto a Windows 2000 (Professional, Server, Advanced Server) con il S.P.2. (Fig. 3).

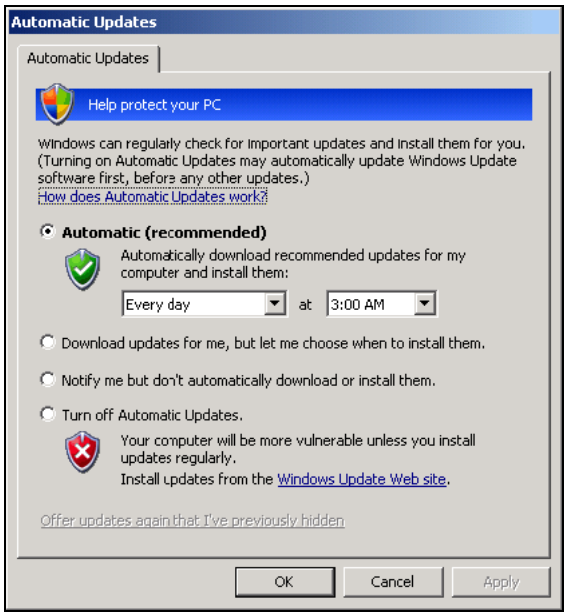

Fig. 3 – Automatic Updates in Windows XP

Il supporto al WSUS è introdotto con SP1 di XP e SP3 di Windows 2000, mentre è automaticamente incluso in Windows Server 2003.
L'*Automatic Update* contatta il servizio Microsoft per i nuovi aggiornamenti ogni 17-22 ore e automatizza il processo di download e installazione per quelli critici. AU valida il server MU e scarica il Download catalog metadata, che utilizza per identificare gli aggiornamenti mancanti. AU notifica all'utente l'operazione in corso, scarica automaticamente gli aggiornamenti utilizzando il servizio BITS e li installa, quindi aggiorna la history e le informazioni di statistica.
Può essere impostato se eseguire l'installazione delle stesse automaticamente oppure essere avvisati quando è disponibile un nuovo aggiornamento.

Office Update

Collegandosi in rete a http://office.microsoft.com/it-it/officeupdate/default.aspx
è possibile verificare l'installazione del pacchetto di Office alla ricerca di patch di sicurezza mancanti o strumenti facoltativi che aggiungono funzionalità ai prodotti Office.
L'utility *Office Update Inventory Tool 2.2* scaricabile dal sito http://www.microsoft.com/office/ork/2003/journ/offutoolv2.htm permette agli amministratori di verificare lo stato degli aggiornamenti di Microsoft Office 2000, Office XP, and Office 2003 per uno o più computer dell'organizzazione.
Da una postazione centrale gli amministratori possono eseguire questo tool, che permette di avere informazioni su quali computer gli aggiornamenti sono installati, quali sono disponibili per essere applicati, quali richiedono un permesso privilegiato di amministratore. L'utility utilizza l'*Office Update Inventory Tool Catalog* (*invcif.exe*) per l'elenco degli aggiornamenti disponibili, scaricabile dal sito http://office.microsoft.com/OfficeUpdate/catalog/inventory/InventoryCatalog.html

Esempi di utilizzo dell'*Office Update Inventory Tool*:
C:\inventory\inventory.exe /s cifs\ /o C:\inventory crea il file nomecomputer.log.
C:\inventory\inventory /update c:\detectionfiles aggiorna il catalogo.
C:\inventory>convert.exe /d C:\inventory /o output.txt .
C.\inventory\inventory /s c:\cifs /o \\computer1\logs
C:\inventory\inventory /s \\computer1\cifs /o \\computer1\logs

Lista dei parametri disponibili:
/s <path> specifica il percorso alla cartella che contiene i file *.cif*
/o <path> specifica il percorso alla cartella di output per il file di log
/update [<path>] aggiorna i file in <path> se necessario.

Per quanto riguarda l'aggiornamento di una installazione centralizzata di Office, viene aggiornata solo l'immagine master di Office a partire dalla quale vengono fatte tutte le altre installazioni del pacchetto; un file *.ini* controlla quali hotfix mancano.

Per lo scanning delle patch di sicurezza per Office può essere utilizzata l'utility *OHotFix*, eseguita localmente su ogni computer e resa disponibile da uno shared server o distribuita come un batch file utilizzando un programma di distribuzione del software tipo SMS ed eseguita ad esempio attraverso il logon script.

Microsoft Baseline Security Analizer

La versione scaricabile gratuitamente dal sito Microsoft è la 2.0, disponibile al sito http://www.microsoft.com/technet/security/tools/mbsahome.mspx.
Può essere utilizzato da utenti Windows Server 2003, Windows XP, Windows 2000 con SP3 o successive.
MBSA controlla la presenza o meno degli update di sicurezza per le seguenti installazioni software:

- Microsoft Internet Information Server 4.0, 5.0 e 6.0;
- Microsoft SQL Server 7.0 e 2000, incluso Microsoft SQL Server Desktop Engine (MSDE) 1.0 e MSDE 2000;
- Microsoft Exchange Server 5.5 e 2000 inclusi i tool di amministrazione di Exchange;
- Microsoft Internet Explorer 5.01 e successivi;
- Microsoft Windows Media® Player 6.4 e successivi.

MBSA riconosce inoltre gli eventuali errori di configurazione presenti nelle applicazioni di Internet Information Server, Internet Explorer, SQL Server, Office 2000 e XP.
MSBA permette inoltre di poter effettuare vari controlli, tra cui i più interessanti sono:

1. *expiration time* delle password degli account
2. tipi di file system e hard driver
3. se l'autologon è attivo
4. se è abilitato l'account Guest

5. RestrictAnonymous registry key settings
6. quanti account di amministratori locali esistono
7. verifica se le password degli utenti locali sono blank o troppo semplici
8. se ci sono servizi non necessari in esecuzione
9. elenca le condivisioni presenti sul compute;
10. se l'auditing è abilitato
11. quale versione di Windows è in esecuzione
12. se è abilitato l'Internet Connection Firewall
13. se è abilitato l'Automatic Update

Le verifiche possono essere fatte confrontando la lista (file *mssecure.xml*) scaricata dal sito Microsoft oppure la lista degli aggiornamenti approvati da un WSUS server.
Per effettuare la scansione di uno o più computer appartenenti ad un workgroup o ad un dominio, server, workstation, l'MBSA offre una GUI o la possibilità di digitare istruzioni a linea di comando si devono possedere i permessi di amministratore locale del computer su cui viene eseguita la scansione (Fig. 4).
Le operazioni di scansione possono essere schedulate utilizzando il comando *mbsacli.exe /hf* ad esempio durante il processo di logon dell'utente, utilizzando un'opportuna Group Policy.
La sintassi del comando mbsacli.exe è la seguente:
mbsacli.exe /hf –h <hostname> -d <domainname> -r <xxx.xxx.xxx.xxx –xxx.xxx.xxx.xxx>
dove: h=nome host della macchina da scansionare,
d=nome del dominio,
r=range di indirizzi ip da scansionare
I risultati delle scansioni eseguite vengono memorizzati in *%userprofile%\SecurityScans*. Viene creato un file per ogni computer scansionato, localmente o remotamente

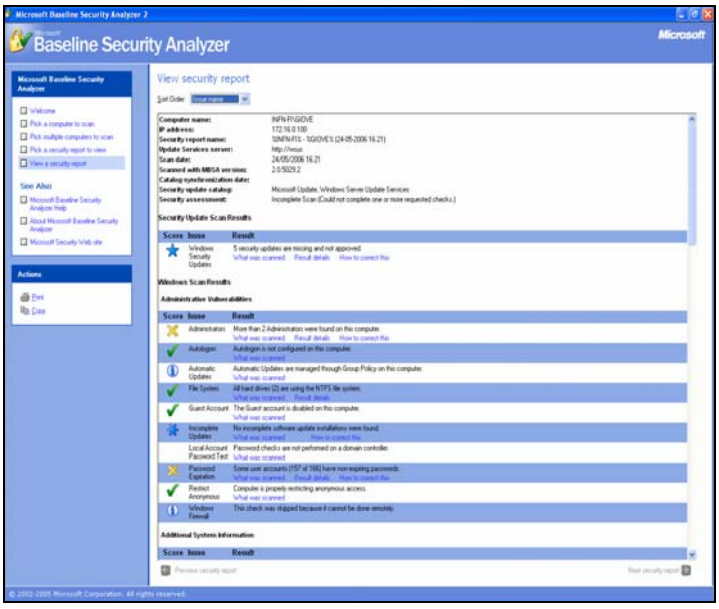

Fig. 4 – Microsoft Baseline Security Analyser

Windows Server Update Services

Windows Server Update Services è la soluzione ideale per gestire e distribuire aggiornamenti critici e patch per sistemi Windows su di una rete di calcolatori di medie dimensioni.
La tecnologia su cui è basato WSUS è quella del Microsoft Update ed è particolarmente adatta a reti Microsoft offrendo la possibilità di integrazione con Active Directory e rendendo sicuri s.o. come Windows 2000 e Windows XP.
WSUS è un tool gratuito scaricabile dal Microsoft Download Center all'indirizzo http://www.microsoft.com/downloads/details.aspx?FamilyID=2478d594-a29c-483c-9dc1-9740bf3081a5&displaylang=en.
Questo strumento permette di ottenere una serie di benefici che lo rendono di sicuro interesse in un ambiente di rete:

- maggior sicurezza, evitando che i singoli client eseguano il download e installino da soli gli aggiornamenti;
- test e approvazione delle patch prima della loro distribuzione automatica;
- notifica dinamica degli aggiornamenti critici ai desktop e server Windows;
- funzionamento anche in presenza di un proxy server che richiede autenticazione;
- aggiornamento dei computer che non possono connettersi direttamente ad Internet;
- conoscenza del livello di sicurezza implementato a livello client;
- maggiori garanzie di privacy.

L'architettura del WSUS è mostrata in Fig. 5.

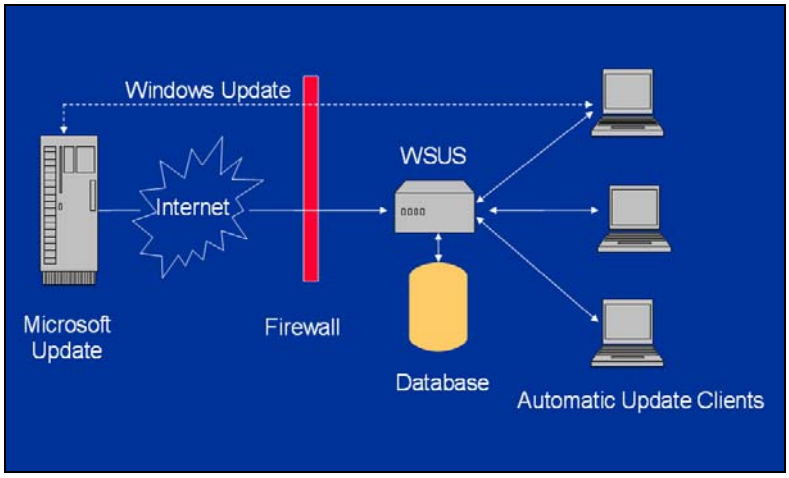

Fig. 5 - Architettura WSUS.

Requisiti e caratteristiche

La componente server del WSUS può essere installata su computer Windows 2000 SP4 e successivi o Windows Server 2003; prerequisiti: IIS 6.0, BITS 2.0, MS .NET Framwork 1.1 s.p. per Win Server 2003. WSUS server fornisce gli strumenti necessari per gestire e distribuire gli aggiornamenti utilizzando il browser IExplorer (non è supportato Mozilla Firefox) e digitando il seguente percorso:

- *http://WSUSInstallationServer:8530/WSUSAdmin*

Un WSUS server (*upstream server*) può essere la sorgente di aggiornamento per altri WSUS server (*downstream server*), in una gerarchia padre-figlio. Il WSUS server che agisce come upstream server deve connettersi al Microsoft Update per scaricare gli aggiornamenti disponibili. L'amministratore stabilisce, sulla base della configurazione e delle opzioni di sicurezza, quanti WSUS server implementare nella propria organizzazione.
La componente client del computer (l'*Automatic Update*), è presente di default in Windows 2000 SP3 e successivi, Windows XP e successivi, Windows Server 2003, Windows Vista e permette al client di ricevere gli aggiornamenti dal WSUS server. WSUS è la versione successiva del Software Update Services (SUS); è basato sulle sue features ma introduce nuove capacità e miglioramenti fra cui:

- aggiornamenti per un numero maggiore di prodotti;
- controllo granulare sugli aggiornamenti da scaricare e installare per prodotto e tipologia;
- supporti linguistici addizionali, UI in italiano;
- introduzione dei gruppi, approvazione degli aggiornamenti personalizzata per gruppo o computer, maggior controllo sul processo di upgrade;
- capacità di verificare se gli aggiornamenti sono appropriati per quel client prima dell'installazione;
- capacità di export/import e di migrazione dei dati;
- API per estendere e personalizzare il pacchetto secondo le esigenze;
- miglior efficienza di consumo di banda attraverso il Background Intelligent Transfer Service (BITS) 2.0, con la possibilità di poter riprendere sincronizzazioni interrotte;
- miglioramento nella reportistica.

Se nella propria organizzazione è già presente un' architettura basata su SUS, per passare a WSUS non è possibile eseguire un update ma va fatta una migrazione utilizzando l'utility:

- *WSUSInstallationDrive:\ProgramFiles\UpdateServices\Tools\WSUSutil.exe*

La tipologia di aggiornamenti supportati riguarda gli aggiornamenti critici, (automaticamente approvati per detection), driver di periferiche, Feature Pack, aggiornamenti di sicurezza (automaticamente approvati per detection), Service Pack,

applicativi, altri tipi di aggiornamenti non critici e non di sicurezza, *Update Rollup.* Non viene fatto il patching di software di terze parti come Acrobat Reader, Firefox ecc.
I prodotti supportati nelle diverse lingue sono:

- Windows XP (32, 64 bit)
- Windows Server 2003 (tutte le edizioni, 32 64 bit)
- Windows 2000 (tutte le edizioni)
- Applicazioni Office 2002/2003/XP (Project, Visio, ecc.)
- SQL Server
- Exchange Server 2003

I requisiti hardware necessari sono mostrati di seguito:

fino a 500 client:

	Minimo	**Raccomandato**
CPU	750 MHz	1 GHz o superiore
RAM	512 MB	1 GB
Database	WMSDE/MSDE	WMSDE/MSDE

da 500 a 15.000 client:

	Minimo	**Raccomandato**
CPU	1 GHz o superiore	dual processor (per n. client > 10.000) a 3 GHz o superiore
RAM	1 GB	1 GB
Database	WMSDE/SQL Server 2000 con SP3a	WMSDE/SQL Server 2000 con Service Pack 3a

Configurazione WSUS client

La configurazione del client WSUS riguarda l'impostazione dei registri di sistema: nel caso di un computer inserito in un workgroup utilizzando la *Local Computer Policy (gpedit.msc)* viene impostata la sezione *Windows Update* presente in *Computer Configuration / Administrative Templates / Windows Components* (Fig 6, Fig. 7).

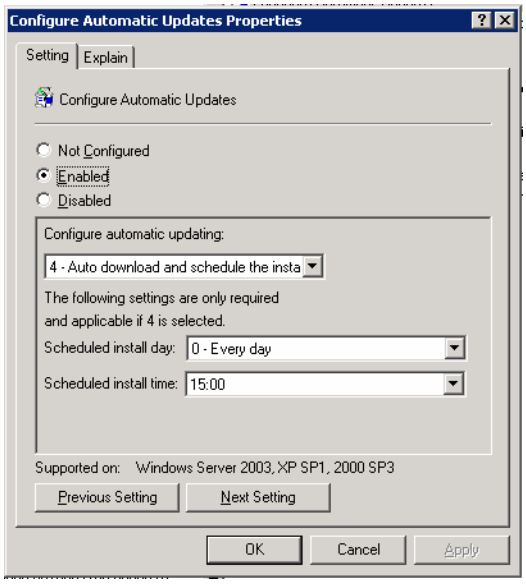

Fig. 6 - Configurazione AU.

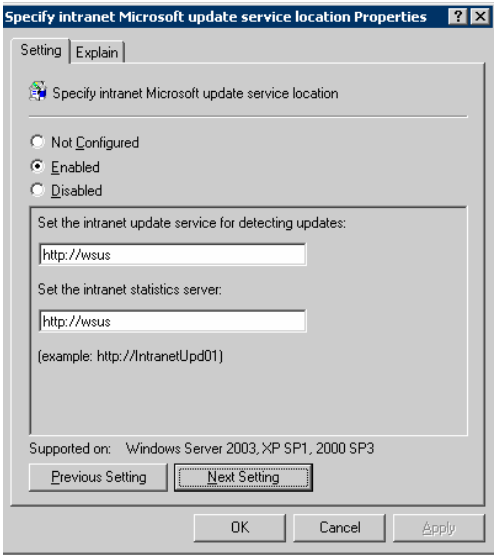

Fig. 7 – Configurazione dell'*Intranet Update Service* in AU.

La stessa operazione può essere eseguita andando direttamente ad interagire con i registri di sistema in:

- *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\ WindowsUpdate*
- *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\ WindowsUpdate\AU*

Una volta effettuata questa impostazione si forza il client ad aggiornarsi e a contattate il WSUS server:

- *gpupdate /force*
- *wuauclt.exe /detectnow*

Nel caso di client inserito in un dominio Active Directory è conveniente impostare la *Group Policy Object* a livello di dominio o di *Organization Unit* (OU).
Una volta configurata mediante policy, le impostazioni locali dell'Automatic Update vengono disabilitate.

L'AU del client esegue un *detection cycle* una volta ogni 17-22 ore verso il WSUS Server; se verifica che esistono nuovi aggiornamenti viene eseguita la scansione del sistema per determinare quali di questi sono applicabili (*Just-in-time validation***)**; viene verificato che Microsoft abbia firmato digitalmente i file e che possano eseguire il download automatico e l'installazione dei Fixes e delle patch di sicurezza solo da parte di utenti con privilegi di amministratore (*Built-in security*). Quindi ne effettua il download in base alle opzioni di configurazione impostate dall'amministratore e utilizzando il servizio *Background Intelligent Transfer Service (BITS)* (*Background downloads***)**, una tecnologia che usa solo la banda non occupata per eseguire i download in modo da non interferire o occupare banda per le altre attività di rete.
Se uno degli aggiornamenti richiede il riavvio del sistema, vengono prima installati tutti e poi fatto ripartire, applicando un singolo restart (*Chained installation***)**.

Configurazione e funzionamento del WSUS server

Una volta installato il pacchetto wsussetup.exe si accede alla sua console amministrativa attraverso un'interfaccia web (Fig. 8) dove vengono mostrati lo stato degli aggiornamenti, dei download e della sincronizzazione nonché l'elenco delle attività da svolgere (verifica aggiornamenti critici, dei computer mancanti, ecc.

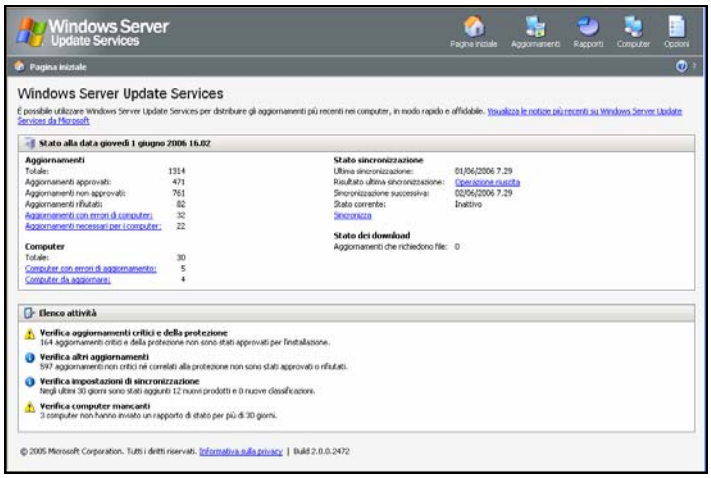

Fig. 8 – Pagina iniziale WSUS server

In maniera semplice dalla pagina iniziale si accede alle pagine degli aggiornamenti, dei rapporti, dei computer, delle opzioni.
La sezione degli aggiornamenti (Fig. 9) è dove si visualizzano tutti gli aggiornamenti scaricati dal Microsoft Update server nel caso di un upstream server; qui si effettua l'operazione di approvazione delle patch: si decide se installarle e su quali gruppi di computer propagarle, oppure rifiutarle. Per ognuno di loro è possibile visualizzarne i dettagli, lo stato, le revisioni. Attraverso un link presente nella sezione dettagli è possibile avere maggiori informazioni collegandosi direttamente al sito della Microsoft sulla specifica patch.

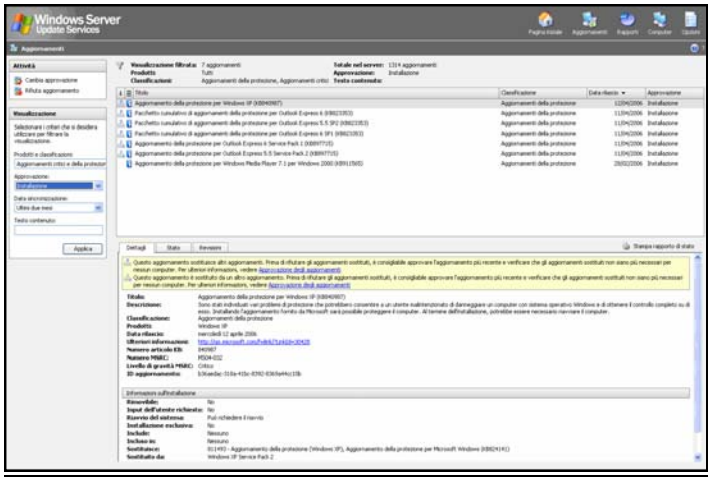

Fig. 9 – Sezione Aggiornamenti.

Nella sezione Rapporti (Fig. 10) sono visualizzati lo stato di tutti gli aggiornamenti per i computer per gruppo di computer (installato, necessario, non necessario, sconosciuto, non riuscito) nonché lo stato degli aggiornamenti per i singoli computer, i risultati della

sincronizzazione (elenco degli update, delle revisioni e degli errori verificatisi durante la sincronizzazione), il riepilogo delle impostazioni correnti presenti nella sezione Opzioni.

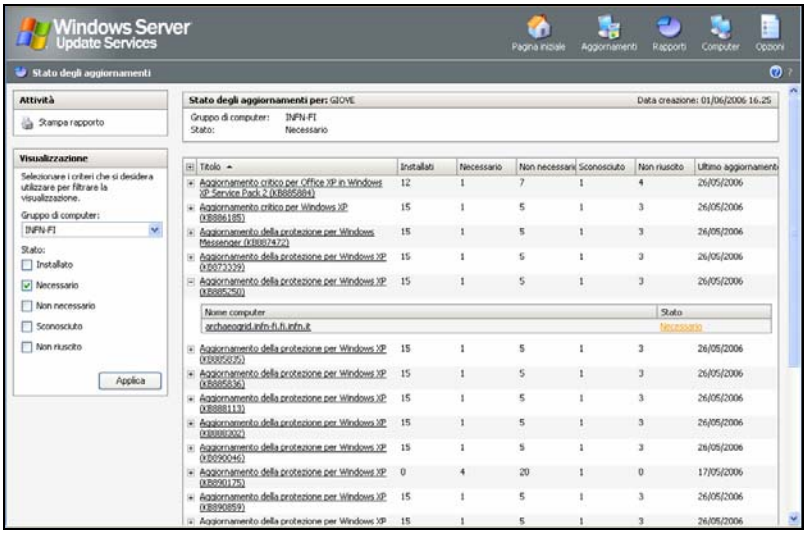

Fig. 10a – Stato degli aggiornamenti nella sez. Rapporti.

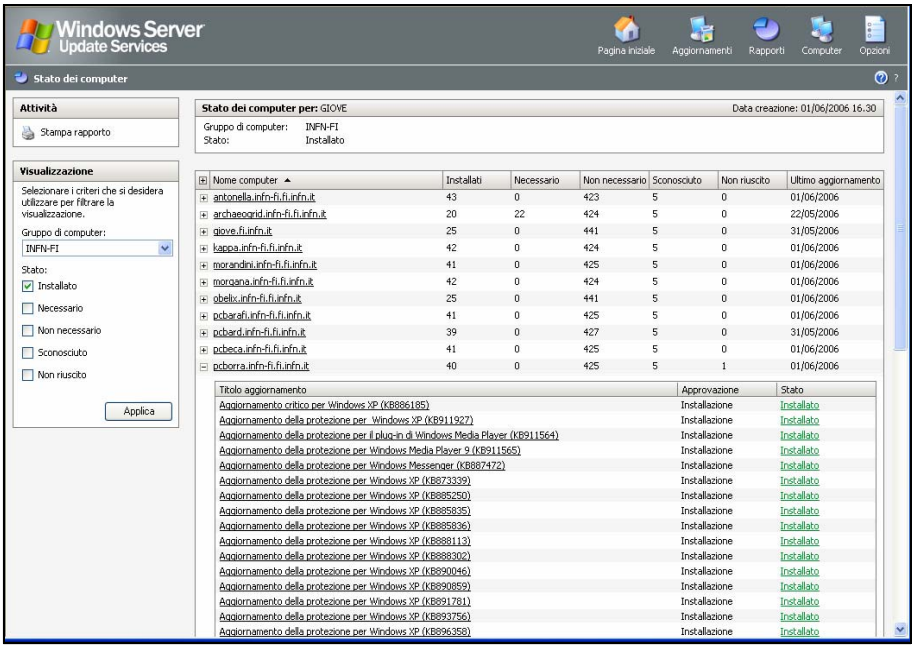

Fig. 10b – Stato dei computer nella sez. Rapporti

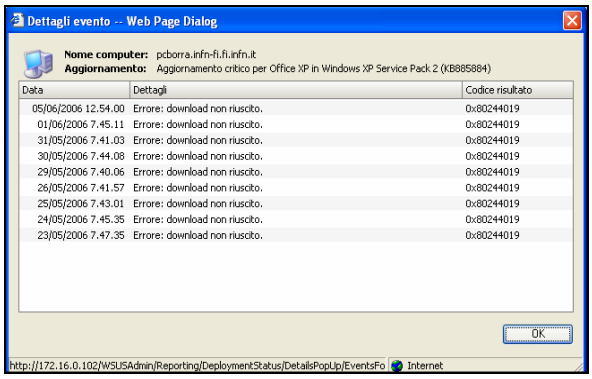

Fig. 10c – Dettaglio evento di un computer nella sez. Rapporti

Nella sezione Computer (Fig. 11) è visualizzato l'elenco di tutti i computer gestiti dal WSUS server. La gestione dei computer può avvenire per gruppo, ossia si possono impostare politiche di approvazione delle patch per gruppo. Ad esempio se viene creato il gruppo dei computer sui quali è installato il sistema operativo Windows 2000, posso definire una politica secondo la quale effettuerò il download e l'installazione per quel gruppo solo delle patch relative a quel s.o., le altre verranno automaticamente scartate dal sistema. Questo criterio permette di risparmiare tempo di download, risorse come lo spazio disco ed eventuali problemi legati alla loro installazione.

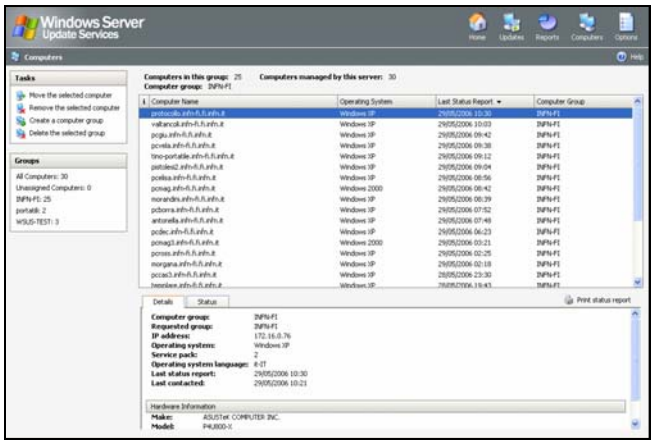

Fig. 11 – Sezione Computer.

Infine nella sezione Opzioni è possibile impostare:

- la sincronizzazione: manuale o schedulata, i prodotti per mi quali si desidera scaricare gli aggiornamenti, la tipologia (aggiornamenti critici, pacchetti di funzionalità, Service Pack, ecc.), se va usato un proxy, se si effettua il download dal Microsoft Update o da un WSUS padre, ecc.
- l' approvazione automatica: si specifica come gestire l'approvazione automatica dell'installazione o del rilevamento degli aggiornamenti per i gruppi selezionati, nonché come approvare le revisioni degli aggiornamenti esistenti;
- la sincronizzazione: come gestire l'assegnazione dei computer ai gruppi, di quali lingue scaricare gli aggiornamenti.

Diagnostica WSUS client e server

Esistono alcuni pacchetti per verificare le impostazioni del WSUS client e server. Il *WSUS Client Diagnostic Tool* (*ClientDiag.exe*) mostrato in Fig. 12 permette di effettuare un check sul client, dalle impostazioni dell'AU al proxy alla verifica della connessione al WSUS server. Analogamente lo script *Check WSUS* (*Check_WSUS_1.05.04.1.vbs*) che si scarica gratuitamente dalla rete effettua controlli sul client (Fig. 13): verifica le impostazioni dell'AU, il WSUS server name, lo stato del WSUS server, il TargetGroup, le Opzioni in accordo con GPO, la modalità autoinstallazione.

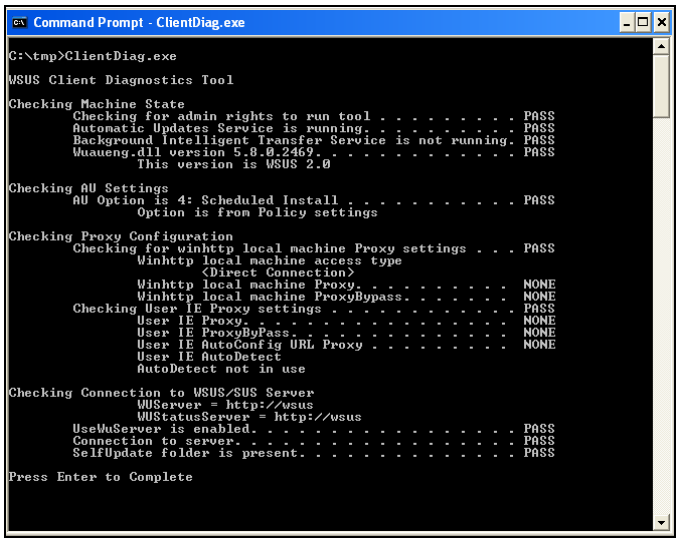

Fig. 12 – Client Diagnostic Tool.

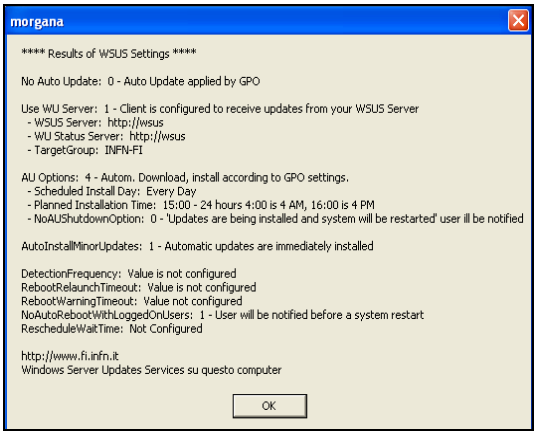

Fig. 13 – Check WSUS.

Invece lato server viene messo a disposizione il *WSUS Server Debug Tool* (Fig. 14):

- *WsusDebugTool [/OutputCab:<value>] /Tool:<value>*

  dove /Tool <value>:

  ResetAnchors
  PurgeUnneededFiles
  ResetForegroundDownload
  GetBitsStatus
  GetConfiguration
  GetLogs
  SetForegroundDownload

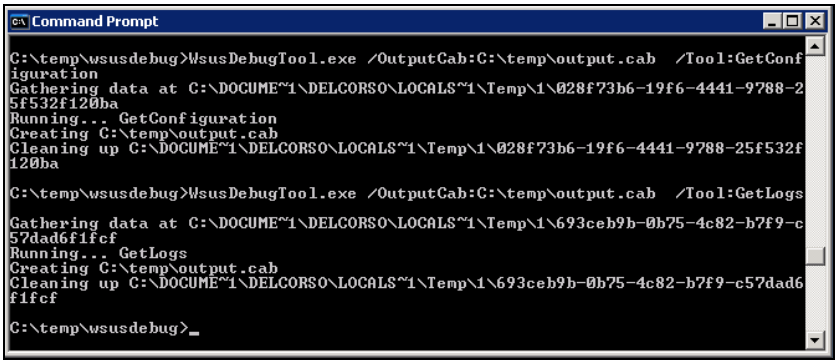

Fig. 14 – WSUS Server Debug Tool.

Ottimizzazione della Performance

WSUS non ha propri parametri direttamente correlati alla performance, ma alcune impostazioni possono migliorare l'efficienza del patching.
Scaricare gli aggiornamenti appena disponibili dal Microsoft Update e non dopo essere stati approvati può essere un metodo; durante la sincronizzazione vengono scaricate solo le informazioni sugli aggiornamenti. Normalmente le patch non vengono scaricate fino a quando non vengono approvate, tranne quelle critiche; poiché appena vengono approvate i client tentano di installarle, se non sono state ancora scaricate il processo si ferma e attende che siano state scaricate.
Un'altra ottimizzazione può essere quella di scaricare i file da installare in modalità express: in questo modo il download e l'installazione degli aggiornamenti nel computer viene eseguito più velocemente, ma questi sono di dimensioni maggiori e pertanto aumentano i tempi di download per il WSUS server dal sito dell'MU.
Utilizzare se possibile un server dedicato per WSUS o quanto meno fare attenzione a quali applicazioni e servizi sono in esecuzione sulla macchina. Può capitare che in presenza di *Share Point Portal Server* sulla stessa macchina il WSUS smetta di funzionare; ai tempi del SUS l'*Internet Printing Protocol* smetteva di funzionare perché l'installazione di SUS metteva il web server in *lockdown*.

System Management Server

Microsoft System Management Server è la soluzione ideale per gestire e distribuire aggiornamenti critici e patch per sistemi Windows su reti di calcolatori di grandi dimensioni, complesse ed eterogenee. Permette di avere un maggior supporto di piattaforma e controllo dei security updates.
Rilasciato nel novembre 2003, SMS 2003 è la soluzione che integra le capacità di patch management del WSUS con quelle di analisi dell'MBSA.
Con SMS possono essere costruiti package da distribuire in maniera mirata, ad esempio per gruppi di computer (laptop, notebook, pc fissi), oppure per diverse versioni del browser IExplorer. Lo strumento è a pagamento.

Ambiente di produzione alla Sez. INFN di Firenze

L'ambiente di produzione attualmente alla Sezione INFN di Firenze è composto da un WSUS server (*Upstream server*) installato su un domain controller con s.o. Windows Server 2003 e SP1, che attraverso una connessione ad Internet scarica dal *Microsoft Update* gli aggiornamenti non appena vengono messi a disposizione da Microsoft. Un secondo WSUS server (*Downstream server*), anch'esso con s.o. Windows Server 2003 e SP1 scarica gli aggiornamenti dal primo (Fig. 14).

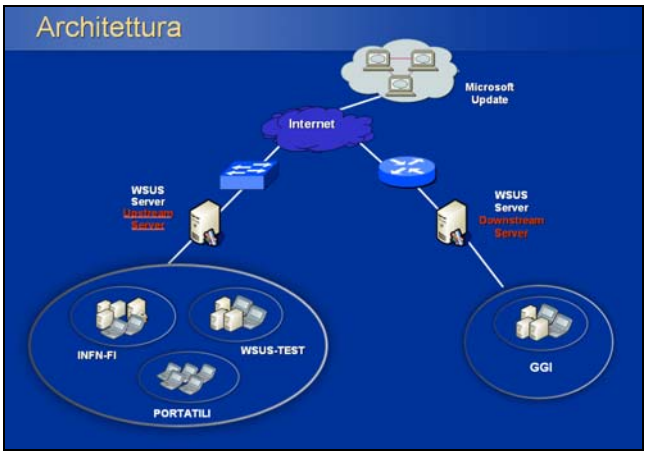

Fig. 14 – Architettura implementata.

Sul WSUS server di sezione sono stati creati 3 gruppi di computer: INFN-FI, WSUS-TEST e PORTATILI, mentre sull'altro al momento c'è solo il gruppo GGI.
In Active Directory dell'Upstraem server è stata creata una Organization Unit WSUS-TEST in cui sono presenti i computer tipo utilizzati per il testing delle patch (s.o. Windows XP Pro + S.P. 1, Windows Server 2003, Windows Vista). Una policy opportuna impostata su questa OU fa sincronizzare i computer di test al WSUS Server che quindi scaricano automaticamente le patch. Esaminando i risultati di tali installazioni e gli eventuali errori prodotti si decide se approvare le patch per gli altri gruppi o meno.
Per indagare più a fondo gli errori prodotti bisogna controllare localmente nell'Event Viewer e nel file *\windows\Windows Update.log* dei client.
Per ogni patch installata nella stessa cartella è presente il relativo file di log; nel caso di problemi da *Control Panel/Add/Remove Program* può essere disinstallata la patch che ha dato errore ed i cui file di disinstallazione sono stati salvati in una cartella nascosta del sistema operativo.
La rimozione centralizzata delle patch dalla console di WSUS non è al momento ancora stata realizzata.
La policy implementata a livello di dominio è mostrata nel Group Policy Manager di Fig. 15.

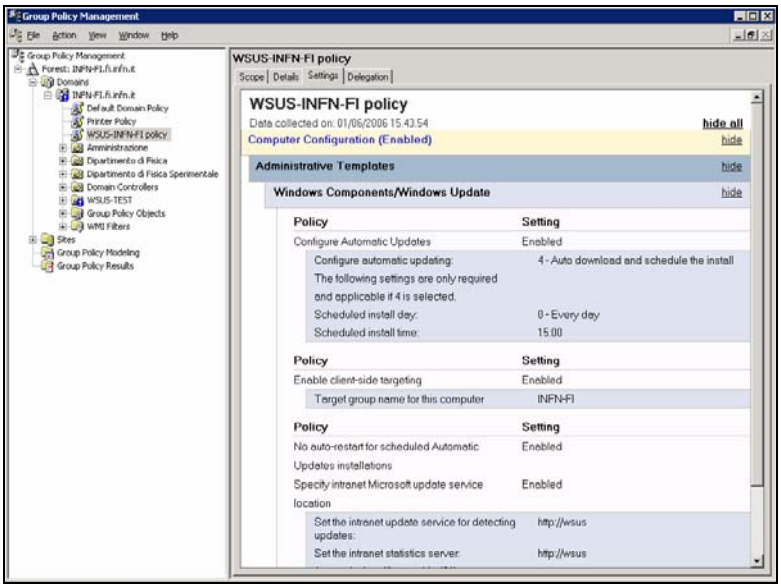

Fig. 15 – WSUS Policy per il dominio INFN-FI

Al momento attuale tutte le macchine nei domini AD sono gestite da WSUS e diverse macchine nei workgroup hanno l'Automatic Update impostato a scaricarsi gli aggiornamenti dal WSUS anziché dal MU.
Le macchine gestite dal WSUS Upstream Server al momento sono :
INFN-FI: 25 client; Portatili: 2; WSUS-TEST: 3 (1 MS Win XP SP2, 1 MS Vista , 1 MS Srv 2003).
Le macchine gestite da WSUS Downstream Server sono:
GGI: 28 client, 1 server.

Conclusioni

WSUS si configura come un valido strumento di Patch Management per tutte le sezioni INFN. E' di facile configurazione e gestione, non ha bisogno di particolari requisiti hardware, è gratuito (per ora :-). Purtroppo si limita a distribuire gli aggiornamenti solo per la piattaforma Microsoft, dal sistema operativo agli applicativi (*Office*, *SQLServer*, *Exchange*, *Windows Defender*), o di terze parti che hanno stipulato accordi commerciali, come Cisco il cui Cisco Trast Agent (CTA) sarà aggiornato in Microsoft Vista attraverso il Windows Update. La possibilità di testare le patch prima del loro rilascio sui pc in produzione permette di monitorare il più possibile gli eventuali problemi legati a questi, mentre una reportistica centralizzata permette di ottemperare agli obblighi di legge secondo i quali deve essere conosciuto lo stato di aggiornamento complessivo delle macchine in rete.

Ringraziamenti

Desidero ringraziare tutto lo staff del Servizio Calcolo e Reti della Sezione INFN di Firenze, il Responsabile Roberto Cecchini per avermi dato piena disponibilità a sperimentare queste nuove tecnologie, nella speranza che lo aiutino a dormire sonni tranquilli lontano da hacker & Co. Un particolare ringraziamento va a Riccardo Veraldi, con cui ho condiviso gioie e dolori oltre ad una valida esperienza lavorativa in Sezione e a cui dedico questa mia pubblicazione.

Documentazione

The Microsoft Guide to Security Patch Management, patterns & practices, Microsoft Corporation, 2003.
Creating a patch and Vulnerability management Program, Mell, Bergeron, Henning, Computer Security Division, NIST, novembre 2005
Deploying Microsoft Windows Server Update Services, Microsoft Corporation, giugno 2005.
Microsoft Windows Server Update Services Operations Guide, Microsoft Corporation, gennaio 2005.
Microsoft Windows Server Update Services Overview, Microsoft Corporation, gennaio 2005.
Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services, Microsoft Corporation, marzo 2005.
Step-by-Step Guide to Migrating from Software Update Services to Windows Server Update Services, Microsoft Corporation, giugno 2005.

Link di riferimento

Microsoft Security site:
http://www.microsoft.com/athome/security/default.mspx
Office Update:
http://office.microsoft.com/it-it/officeupdate/default.aspx
MBSA:
http://www.microsoft.com/mbsa
WSUS:
http://www.microsoft.com/wsus
Microsoft Windows Server Update Services Overview:
http://go.microsoft.com/fwlink/?LinkID=42213
Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services:
http://go.microsoft.com/fwlink/?LinkID=41774
Deploying Microsoft Windows Server Update Services:
http://go.microsoft.com/fwlink/?linkid=41777
Platform SDK WSUS:
http://go.microsoft.com/fwlink/?LinkID=43101

WSUS Communities
http://www.wsuswiki.com
http://blogs.technet.com/WSUS/