Windows avanzato

Versione 1.1 del 20/12/2005

Premessa

Questo documento contiene alcune raccomandazioni che un Amministratore di Sistema MS Windows dovrebbe seguire per aumentare la sicurezza informatica di un computer. In particolare, il documento è dedicato agli **amministratori di Windows NT/2000/XP**.

Si ricorda che Microsoft ha da tempo congelato e archiviato gli aggiornamenti critici per il sistema operativo Windows NT, motivo piu' che sufficiente per abbandonarlo.

Oltre ad alcune raccomandazioni generali, gli aspetti che saranno trattati riguardano l'installazione e la gestione del sistema operativo, il monitoraggio dell'uso, il backup, l'uso di antivirus e di personal Firewall.

Raccomandazioni generali

Antivirus e antispyware:

E' cura dell'amministratore l'installazione di un sistema antivirus e di un sistema antispyware. "Spyware" sono i programmi che penetrano nel computer per reperire informazioni all'insaputa dell'utilizzatore.

I Servizi di Calcolo e Reti dispongono di software e licenze e sono in grado di prestare consulenza al riguardo.

Si raccomanda di abilitare l'aggiornamento automatico del prodotto e la protezione in tempo reale.

Account e password:

Non utilizzare utenze con privilegi se non strettamente necessario, in particolar modo per la gestione remota: è obbligatorio l'uso di applicazioni basate su protocolli criptati.

Definire un tempo di validità delle password, che siano formate almeno da 8 caratteri, basate su numeri, lettere e caratteri.

Disabilitare l'opzione di memorizzazione della password in sistemi automatici.

Disabilitare l'autenticazione LanMan (ancora presente per compatibilità con i sistemi Windows 9x), che consiste nella traduzione delle password in un formato più semplice da violare rispetto al sistema NTLM di Windows 2000, modificando la chiave:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
LMCompatibilityLevel REG_DWORD = 5
```

Impedire l'accesso remoto al Registry da parte di utenti non amministratori, modificando la chiave in:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

secondo le indicazioni riportate in Microsoft Knowledge Base Article – 153183 [ref. 4].

Per Windows XP, se è stato attivato un account di default facente parte del gruppo di amministratori, ma diverso da Administrator, ricordarsi di disabilitare l'account Administrator, poiché questo risulta ancora attivo e senza password.

Condivisione di risorse:

Abilitare la condivisione delle directory solo quando necessario, impostando sempre le opportune restrizioni.

Servizi:

Non avere installati, anche se *stopped*, eventuali servizi non necessari (es. *telnet*).

Se l'host fornisce servizi centralizzati (ad es. WWW, DNS, FTP, ecc.) si raccomanda la lettura del documento specifico [ref. 1].

Verificare in particolare la configurazione e l'aggiornamento di IIS (Internet Information Services) [ref. 2] e di SQL Server [ref. 3], se installati.

Firewall:

Assicurarsi che sui border router o firewall presenti siano implementati filtri per le porte 135, 137, 138, 139 e 445. Rimuovere i protocolli non necessari, quali ad esempio NetBeui, IPX.

Valutare inoltre l'opportunità di attivare un personal Firewall, secondo le modalità indicate dal locale Servizio di Calcolo e Reti.

Domini e Active Directory:

La configurazione di Active Directory o altri domini Windows deve essere coordinata con i Servizi di Calcolo e Reti locali.

File System:

Preferire il file system NTFS a FAT o FAT32, poiché permette di definire la politica di accesso ai file e ottimizza le performances.

Aggiornamenti e *patch* di sicurezza

Tutti i sistemi operativi evidenziano nel tempo bachi di sicurezza e nuove vulnerabilità. Per le vulnerabilità scoperte all'interno di Windows 2000 e di Windows XP la Microsoft ha provveduto a rilasciare apposite patch risolutive, prelevabili dal suo sito web od autoinstallanti ricorrendo al servizio Windows Update. Più in generale, Microsoft ha rilasciato, per le varie versioni di Windows, numerosi **Service Pack.** I Service Pack sono, essenzialmente, un unico archivio contenente la raccolta di tutte le patch per quella specifica versione di Windows, in grado di risolvere problemi di sicurezza, comportamenti inattesi in determinate circostanze hardware/software di utilizzo, problemi minori relativi all'interfaccia utente.

Installare subito le patch più recenti per Internet Explorer

Uno degli aggiornamenti che è consigliabile effettuare immediatamente dopo l'installazione del Service Pack, consiste nel prelievo e nell'installazione delle ultime patch per Internet Explorer.

Windows update

E' disponibile una funzione (Windows update) che consente di individuare gli aggiornamenti e di scaricarli automaticamente nel computer. Sono impostabili livelli diversi, che consentono di essere avvisati preventivamente o permettono l' aggiornamento secondo una pianificazione specificata.

Si raccomanda di ripetere il controllo presso il sito di Windows Update fino a che il sistema non risulti completamente aggiornato.

"Microsoft Update" consente di aggiornare, oltre al sistema operativo, anche gli altri prodotti del medesimo produttore, se installati. (Office, etc.)

MBSA

Microsoft ha rilasciato un'utilità gratuita denominata **Microsoft Security Baseline Analyzer (MBSA)**, specificamente sviluppata per sistemi Windows 2000 e Windows XP, che si occupa di controllare lo stato del sistema operativo e di proporre il download delle ultime patch disponibili.

Si differenzia dall'uso di Windows Update per il livello di aggiornamento più tempestivo: MBSA è spesso in grado di informare circa l'uscita di patch ed aggiornamenti che possono essere inseriti in Windows Update anche con settimane di ritardo.

Con l'esecuzione di MBSA viene prodotto un sommario dettagliato secondo le direttive di controlli da effettuare impostati.

Network Security Hotfix Checker

Per Windows 2000 e NT, IIS 4.0 e 5.0, IE e SQL server è disponibile il tool Microsoft Network Security Hotfix Checker (Hfnetchk.exe) che permette all'amministratore di verificare se sono state installate tutte le patches di sicurezza disponibili [ref. 5].

Monitoring

Abilitare l'audit per eventi quali ad esempio logon/logoff ed essere sicuri che nell'event log siano riportate le segnalazioni di tentativi di accesso non autorizzati.

Verificare periodicamente i log e mantenerne una copia.

REFERENZE

[1] Servizi Centralizzati

[2] NSA Security Guides (IIS: sd-3, sd-4, sd-7, w2k-, wxp-, wnt-security-guides)

[3] NSA Security Guides (SQL: sd-9)

[4] Microsoft Knowledge Base Article – 153183
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q153/1/83.asp&NoWebContent=1

[5] Microsoft TechNet**: HFNetChk**
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp

Risorse disponibili in rete

Microsoft http://www.microsoft.com/italy/security/

NSA Security Recommandation Guides http://www.nsa.gov/snac/

SANS Institute "The twenty most critical internet security vulnerabilities".

http://www.sans.org/top20/ (versione originale aggiornata)

http://www.datasecurity.it/top20/Top20-2003.html (traduzione italiana)