La gestion des correctifs de sécurité dans un parc Windows : des solutions techniques à la mise en œuvre pratique en entreprise

Patrick Chambet (Edelweb)
Eric Larcher (Accor Services)

Introduction

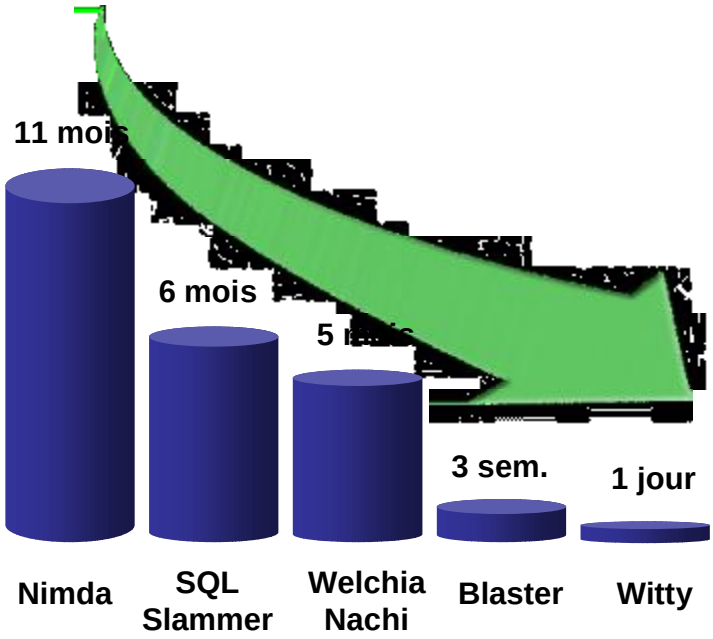
La gestion des correctifs de sécurité (plus communément appelés « patches ») est l'une des tâches les plus ingrates des équipes d'administration et de sécurité des entreprises. Pourtant, nul ne peut s'y soustraire sans que des conséquences importantes en découlent.

En effet, il y a encore quelques années, la gestion des patches n'était nécessaire que sur un sous-ensemble restreint de systèmes : principalement les serveurs les plus sensibles et/ou exposés (serveurs joignables depuis Internet par exemple). Ce faisant et en appliquant quelques règles de sécurisation de bon sens, on évitait d'offrir sur un plateau des cibles de choix pour les pirates du dimanche et autres « scripts-kiddies ».

Malheureusement, aujourd'hui, ce n'est plus aussi simple. La cause, il faut la chercher du coté des virus et autres vers auto-propagateurs principalement. La menace a en effet évolué et s'est même automatisée avec l'apparition de vers exploitant des failles de sécurité de logiciels largement répandus sur le marché pour pénétrer les systèmes non patchés, tels CodeRed, Nimda et autres Blaster. Pire, le périmètre vulnérable s'est considérablement élargi : il ne suffit plus de protéger les serveurs sensibles ou exposés dont on parlait plus haut, car toute machine (tel le PC d'un utilisateur lambda) est source potentielle de contamination. L'impact unitaire n'est, il est vrai, que de faible intensité, mais lorsque des centaines, voire des milliers de PC sont infectés par des vers balayant des plages d'adresses entières à la recherche de machines vulnérables, c'est le réseau interne (LAN voire WAN) de l'entreprise qui fait grise mine. Sans parler des éventuels effets de bord des vers ou virus en question (destruction de fichiers, diffusion de documents confidentiels situés dans le répertoire « Mes Documents » ou sur le Bureau à tout le carnet d'adresses, etc.).

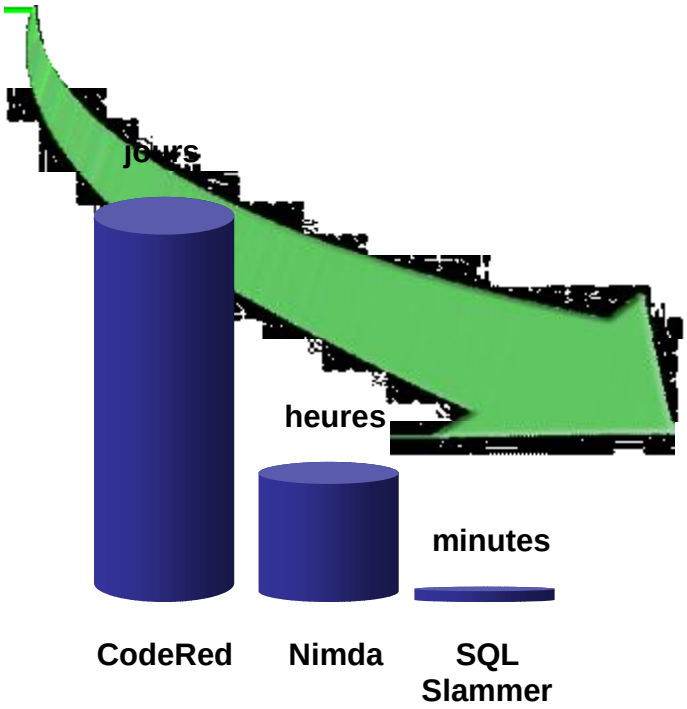
L'étude des principaux vers ayant affecté les entreprises du monde entier durant ces dernières années montre par ailleurs que la situation ne fait qu'empirer.

En effet, de Nimda à Blaster par exemple, la période de gestation des vers (entre la publication de la vulnérabilité par l'éditeur concerné et l'apparition d'un ver exploitant la faille en question) s'est considérablement raccourcie : 11 mois pour Nimda, 6 mois pour SQL Slammer et seulement trois semaines pour Blaster (on peut même citer Witty, affectant les produits ISS : 1 journée !).



Intervalle entre la révélation d'une nouvelle vulnérabilité et son exploitation par un ver

De plus, la vitesse de propagation des vers (entre l'apparition des premières instances du ver et l'atteinte du nombre maximal de machines contaminées) s'accélère : quelques jours pour CodeRed, quelques minutes seulement pour SQL Slammer :



Vitesse de propagation de quelques vers

En clair, il est urgent d'*agir* si l'on ne veut pas passer son temps (et son argent) à *réagir* en cas de contamination. Une solution consiste à définir une politique de gestion des correctifs adaptée à la menace du moment et aux contraintes métier de l'entreprise et à l'implémenter à l'aide des outils disponibles sur le marché. Nous allons donc, dans cet article, commencer par un panorama des outils de gestion des correctifs de sécurité dans un environnement Windows avant de présenter un exemple de mise en œuvre au sein d'une entreprise du secteur tertiaire.

Les outils de gestion des correctifs

Comme indiqué plus haut, il apparaît aujourd'hui indispensable de mettre en place une politique de gestion des patches au sein de toute entreprise. Cependant, les approches classiques, basées sur des actions manuelles ou semi-automatiques (comme Windows Update) ne sont pas suffisantes à l'échelle d'une entreprise. La gestion des patches doit donc être automatisée de façon à faciliter le suivi de leur application, à être réactif en cas d'apparition d'une nouvelle menace (nouvelle attaque par exemple), à les tester avant leur déploiement et à faciliter le retour en arrière en cas de problème.

Une politique type de gestion de patches

Une politique type doit pouvoir répondre à un certain nombre de questions et, notamment : qui ? quoi ? quand ? où ? et comment ?

Qui : Seuls les administrateurs (ou les processus tournant avec des droits d'utilisateur ayant de hauts privilèges) devraient avoir l'autorisation d'installer des patches sur un ordinateur. Les utilisateurs ne doivent pas effectuer eux-mêmes ce type d'opération, notamment sur leurs postes de travail.

Quoi : seules les mises à jours officielles des éditeurs devraient être appliquées. La vérification de leur origine est impérative. De plus, les administrateurs doivent tester et approuver les correctifs tout en rejetant ceux qui sont inutiles dans le contexte de la société ou qui peuvent être dangereux (effets de bords néfastes pour la bonne marche du SI).
Une sélection automatique des patches nécessaires (parmi ceux qui ont été approuvés) doit être faite, en fonction de la version du système d'exploitation du système cible : il va sans dire qu'on n'installera pas de patches Windows 2000 sur un système Windows XP.

Quand : les patches doivent être appliqués automatiquement mais de façon coordonnée. Par exemple, Microsoft recommande d'appliquer les patches critiques sous 24 heures, ceux classés « importants » sous un mois, ceux concernant une faille d'importance « modérée » sous 4 mois et les autres (faible importance) sous un an…

Où : sur la totalité des ordinateurs. Même les PC portables doivent être patchés. C'est la raison pour laquelle il est impératif qu'ils se reconnectent régulièrement au réseau de l'entreprise.
D'où les correctifs doivent-ils être téléchargés ? Depuis un ou plusieurs serveurs centraux, en utilisant typiquement le plus proche.

Comment : les patches sont appliqués automatiquement, en tâche de fond, de façon à ce que l'opération soit transparente pour l'utilisateur. Si nécessaire, un redémarrage du système devra être planifié. Des informations pertinentes doivent être enregistrées dans des logs pendant et après l'opération.

Une telle politique de gestion de patches peut être implémentée à l'aide de certains outils diffusés par Microsoft. Nous allons maintenant analyser certains de ces outils.

MBSA

MBSA (Microsoft Baseline Security Analyzer) est l'un des outils Microsoft les plus simples. Il est issu à l'origine de la société Shavlik. Une version gratuite de cet outil peut être téléchargée à l'URL suivante :

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

La dernière version générique de MBSA est la 1.2, mais une nouvelle version, la 1.2.1, est nécessaire afin de pouvoir être compatible avec le SP2 de Windows XP : il offre une meilleure intégration avec les améliorations de sécurité du SP2.

MBSA 1.2.x peut effectuer des scans en local ou à distance sur des systèmes Windows NT 4.0, Windows 2000, Windows XP, et Windows Server 2003. En plus des patches de sécurité Windows, il supporte également un grand nombre de produits Microsoft :

- IIS 4.0, 5.x, 6.0
- SQL Server 7.0, 2000
- IE 5.01+
- Exchange Server 5.5, 2000, 2003
- Windows Media Player 6.4 et plus
- Microsoft Office (scans locaux seulement)
- MDAC 2.5, 2.6, 2.7, and 2.8
- Microsoft Virtual Machine
- BizTalk Server 2000, 2002, 2004
- Commerce Server 2000, 2002
- Content Management Server 2001, 2002
- Host Integration Server 2000, 2004, and SNA Server 4.0.

MBSA peut être exécuté en mode graphique (lancer `mbsa.exe`) ou en ligne de commande (lancer `mbsacli.exe`). Dans le second mode, il est possible d'utiliser des

fichiers batches afin d'automatiser l'outil. Par exemple, le script qui suit scanne un système et enregistre les résultats dans un fichier XML :

```
set cname=%computername%
set uname=%username%
"C:\Program Files\MBSA\mbsacli.exe" /nvc /nosum /c %cname% /n
  IIS+OS+SQL+Password /o %cname%
copy "%userprofile%\SecurityScans\%cname%.xml"
  "\\%cname%\c$\Documents and Settings\%uname% \SecurityScans\"
```

MBSA remplace les anciens outils HFNetChk et MPSA. Afin d'émuler le mode de fonctionnement de HFNetCheck, on peut lancer MBSA avec les paramètres suivants :

```
mbsacli.exe -hf -?
```

Comment MBSA fonctionne-t-il ?

Voici les différentes étapes du processus de vérification de MBSA lorsqu'il est lancé :

1 – MBSA analyse la configuration de sécurité du système analysé. Il détecte les erreurs de configuration les plus fréquentes telles que :

- Les partitions en FAT
- Les comptes Administrateurs
- Les mots de passe triviaux
- Les services activés qui peuvent être dangereux
- Les partages de fichiers
- La politique d'audit
- La configuration du Firewall ICF (en local uniquement)
- Etc.

Pour une liste complète des tests de sécurité effectués par MBSA, se reporter au fichier `Checks.csv` situé dans le répertoire de MBSA.

2 – MBSA télécharge ensuite une référence de sécurité au format XML : il s'agit en fait d'un fichier nommé mssecure.xml. MBSA peut télécharger ce fichier directement depuis Internet ou à partir d'un serveur MSUS interne.

Depuis Internet, MBSA essaye successivement les liens suivants :

http://go.microsoft.com/fwlink/?LinkId=18922
http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab (*version 3.32*)
http://www.microsoft.com/technet/security/search/mssecure.xml

Le fichier CAB contient une version compressée du fichier mssecure.xml.
Notez qu'il est également possible de télécharger le dernier référentiel de sécurité à partir des liens suivants sur le site de shavlik :

http://xml.shavlik.com/mssecure.cab (*version 4.0*)
http://xml.shavlik.com/mssecure.xml

Si MBSA ne peut pas télécharger le fichier mssecure.xml, il utilise la copie locale (la dernière version téléchargée en local). Ainsi, vous pouvez télécharger le fichier mssecure.xml de Shavlik et l'utiliser avec MBSA ! Mais notez que c'est une opération non supportée par Microsoft.

3 – Puis MBSA analyse le niveau de patches du système scanné par rapport au référentiel de sécurité.

4 – MBSA détecte les patches de sécurité manquants, ainsi que les Service Packs, et affiche les messages correspondants dans son rapport.

Le fichier mssecure.xml est un fichier précieux : il contient tous les correctifs de sécurité publiés depuis 1998, avec des informations descriptives. Pour chaque patch, sont indiquées notamment les informations suivantes :

- Description
- Chemin d'accès au fichier de mise à jour
- Chemin, version et somme de contrôle du patch
- Les clés de registre modifiées par le patch.

Le fichier mssecure.xml contient aussi un historique des anciens correctifs inclus depuis dans des patches cumulatifs ou des Service Packs. Ce fichier XML est bien sûr modifié à chaque fois qu'un nouveau correctif de sécurité est publié.

Les limites de MBSA

MBSA a tout de même certaines limites. Par exemple, quand il ne peut pas confirmer de façon sure qu'un patch a été appliqué, il indique un message de type "Note". Cela arrive quand des produits n'ont pas de critères de détection (MSXML pour le patch MS02-008 par exemple) ou quand il y a plus d'un patch pour un même produit selon l'OS utilisé (c'est une limite du schéma XML de mssecure.xml). Dans le cas de DirectX 9.0 pour Windows 2000 / XP / 2003 (MS03-030) par exemple, on obtient :

```
Note   MS03-030   Q819696
Please   refer   to   http://hfnetchk.shavlik.com/support   for   a
detailed explanation.  Refer to the section on Note Messages.
```

Parfois, MBSA ne peut que vérifier la valeur de certaines clés de registre afin de déterminer si un patch est installé ou non. Par exemple, dans le MS03-037, des clés de registre communes sont présentes pour chaque version de vbe6.dll mais les versions ou les sommes de contrôle sont différentes :

```
Patch NOT Installed      MS03-037        Q822150
File C:\Program Files\Common Files\Microsoft
```

```
Shared\VBA\VBA6\vbe6.dll has an invalid checksum and
its file version [6.4.99.69] is equal to what is
expected [6.4.99.69].
```

Quand un patch qui n'est pas un correctif de sécurité écrase des fichiers précédemment patchés, MBSA indique les fichiers corrigés comme étant non sûrs :

```
Warning                  MS03-023        Q823559
File C:\Program Files\Common Files\Microsoft
Shared\TextConv\msconv97.dll has a file version
[2003.1100.5510.0] greater than what is expected
[2003.1100.5426.0].
```

Par ailleurs, la langue par défaut de l'ordinateur analysé détermine aussi si les tests de checksums sont effectués ou non (options /hf, /sum et /nosum).

Scripter MBSA

Les scans de MBSA peuvent être automatisés en utilisant des scripts : vous pouvez ainsi réaliser des tests à large échelle ainsi que permettre à des utilisateurs ayant des privilèges réduits de vérifier eux-mêmes leur niveau de sécurité sans avoir besoin d'appeler le service informatique. Pour plus d'information, voir :

http://www.microsoft.com/technet/security/tools/mbsascript.mspx

Vous pouvez par exemple télécharger les scripts batchscan.js et rollup.js, qui permettent de scanner un nombre illimité de systèmes ou d'adresses IP à partir d'un fichier, tout en compilant les résultats dans un rapport de synthèse unique (fichier XML) qui peut être visualisé à l'aide d'Internet Explorer.

Windows Update

Windows Update est un outil de vérification et d'installation en ligne de patches qui peut être utilisé selon deux modes : un mode manuel, avec Internet Explorer pointant sur l'adresse http://windowsupdate.microsoft.com, et un mode automatique, utilisant le service « Automatic updates » comme partie cliente. Windows Update est idéal pour les compagnies de petite taille.

Lorsqu'il est utilisé en mode automatique, le service "Automatic Updates", qui permet une mise à jour automatique et en tâche de fond, nécessite que le service BITS (Background Intelligent Transfer Service) soit activé : ce service utilise la bande passante non exploitée afin de télécharger les patches depuis le site Web de Microsoft, de façon à rendre le processus totalement transparent pour l'utilisateur.

Windows Update n'utilise pas le même mécanisme que MBSA. Le client WU vérifie que chaque patch a été correctement installé sur l'ordinateur local. Pour ce faire, il effectue des vérifications à plusieurs niveaux :

- Clés de registre (situées dans `HKLM\SOFTWARE\Microsoft\Updates\Windows` *`[VERSION]`*`\SP`*`[X]`*`\KB`*`xxxxxx`*)
- Liste de fichiers sur le disque
- Version et somme de contrôle de ces fichiers.

Le processus de mise à jour tourne en tâche de fond et reste transparent pour un utilisateur normal. Les notifications de nouveaux patches sont présentées à l'utilisateur logué localement seulement s'il a les privilèges Administrateur :

Ce type de notification a exactement le même aspect qu'avec le client MSUS (voir ci-dessous).

Microsoft Software Update Service

Microsoft Software Update Service (MSUS) est un outil gratuit qui peut être téléchargé à l'URL suivante :

http://www.microsoft.com/windowsserversystem/sus/default.mspx.

Contrairement à MBSA, qui peut vérifier plusieurs produits Microsoft, MSUS ne gère actuellement que les correctifs Windows. Il ne gère pas les applications pour le moment, mais la prochaine version (2.0) de MSUS devrait corriger cette limitation.

Le principe de MSUS est d'avoir un serveur « Windows Update dans votre société » : un ou plusieurs serveurs internes hébergent les patches de sécurité. A chaque fois que de nouveaux correctifs de sécurité sont publiés, l'administrateur approuve les patches

nécessaires. Ensuite, les postes utilisateurs se connectent automatiquement à l'un des serveurs internes de façon à télécharger et appliquer les patches validés.

Remarque : contrairement à WindowsUpdate, MSUS ne vérifie pas le numéro de série des logiciels installés…

MSUS utilise une interface d'administration Web (http://sus.votre-intranet.com/SUSAdmin/) et a besoin d'IIS sur les serveurs MSUS internes. Les outils IISLockdown et URLScan sont automatiquement installés sur ces serveurs IIS durant le setup de MSUS afin de les sécuriser.

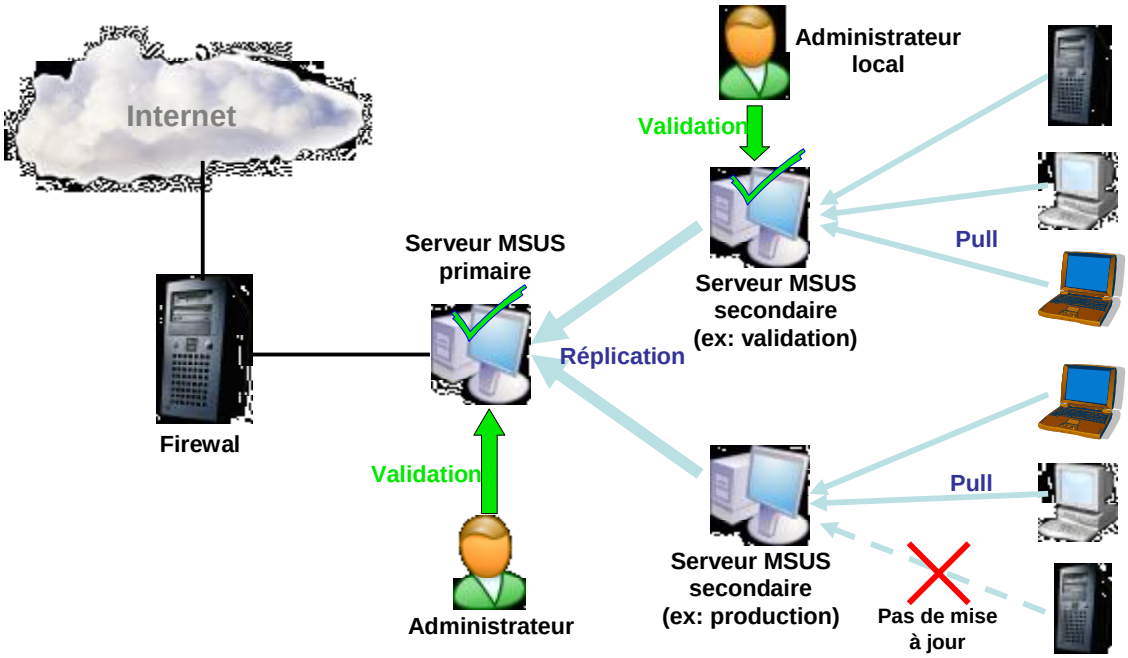
Comment MSUS fonctionne-t-il ?

MSUS fonctionne un peu comme MBSA, même si leurs formats sont différents : MSUS a aussi besoin d'un référentiel de sécurité. Chaque jour, MSUS effectue un processus de synchronisation, en suivant les étapes ci-dessous :

- MSUS télécharge un référentiel de sécurité (fichiers XML) situé à:
  - http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab
  - http://www.msus.windowsupdate.com/msus/v1/aurtf1.cab
- Il valide la signature de Microsoft sur les CABs
- Il compare ce référentiel au contenu de sa base locale de façon à identifier les nouvelles mises à jour
- Il télécharge les nouveaux patches et vérifie leur signature
- Il met à jour ses journaux de synchronisation et d'approbation
- Si la synchronisation programmée échoue, SUS réessaye trois fois avec à 30 minutes d'intervalle.

Les administrateurs doivent alors approuver les nouvelles mises à jour avant qu'elles ne puissent être appliquées sur les ordinateurs du réseau local.

Une architecture MSUS avancée ressemble à ceci :



Après approbation des patches par l'administrateur, les mises à jour peuvent être dans l'un des états suivants :

- New (aucun choix n'a été fait par l'administrateur)
- Approved (approuvé)
- Not approved (non approuvé)
- Updated (une nouvelle version du patch vient d'être téléchargée. Il s'agit d'une sorte de "méta-patching" ou patch d'un patch)
- Temporary unavailable (le patch associé n'est pas disponible ou une dépendance n'a pas été trouvée).

Notez qu'un correctif qui a déjà été appliqué et qui est ensuite marqué « not approved » par un administrateur ne pourra plus être désinstallé par le client AutoUpdate. Cela ne sera plus le cas avec WUS (Windows Update Services, le nouveau nom MSUS version 2.0) qui sera capable de désinstaller des patches précédemment appliqués.

MSUS est un outil très puissant qui permet d'implémenter la politique typique que nous avons présentée précédemment en répondant aux différentes questions posées :

Qui : le service « Automatic Updates » tourne avec les privilèges SYSTEM. Si un utilisateur est Administrateur, il a le choix d'appliquer ou pas les patches (voir plus haut). Les utilisateurs normaux ne peuvent pas refuser l'application automatique des patches, mais ne peuvent pas installer des patches de leur propre initiative.
D'ailleurs, une fois que MSUS est installé sur votre réseau interne, il est recommandé d'appliquer des règles de filtrage sur votre Proxy HTTP sortant. Les sites à autoriser pour le serveur SUS primaire sont les suivants :

http://www.msus.windowsupdate.com
http://download.windowsupdate.com

http://cdm.microsoft.com

De plus, les sites à interdire pour tout autre système (serveurs et stations de travail), de façon à éviter l'installation manuelle de correctifs par les utilisateurs, sont les suivants:

http://www.windowsupdate.com
http://windowsupdate.microsoft.com

Quoi : MSUS ne peut installer que les patches de sécurité de Windows, c'est-à-dire les correctifs de sécurité, les SRP (Security Rollup Packages), les mises à jours critiques de Windows ainsi que les Service Packs.
Le serveur SUS vérifie la signature des mises à jour afin d'être sûr qu'ils ont bien été émis par Microsoft. Les mises à jour appropriées sont alors automatiquement sélectionnées (parmi celles qui ont été validées par l'administrateur), en fonction de l'ordinateur cible (version de l'OS, langue, etc.). MSUS supporte des mises à jour en 31 langues.

Quand : les patches sont appliqués automatiquement chaque jour, à une heure précise que vous pouvez définir. Un délai aléatoire entre les différents clients permet d'éviter des connexions simultanées sur le serveur SUS. Les patches sont aussi appliqués au moment du démarrage, si l'heure spécifiée est dépassée.

Où : les patches sont appliqués sur chaque ordinateur ayant le client Automatic Updates configuré. Un « pull » HTTP est utilisé afin de récupérer les mises à jour depuis le serveur MSUS.

Comment : les mises à jour sont d'abord testées et approuvées par l'administrateur. Ensuite, les correctifs sont transférés entre le serveur SUS principale et les serveurs SUS secondaires, puis vers les clients, en tâche de fond, en optimisant la bande passante grâce au service BITS. Puis les patches sont automatiquement appliqués sur chaque ordinateur, en tâche de fond ou non. Si nécessaire (dans 30% des cas environ), un unique redémarrage est effectué. Enfin, les journaux de synchronisation et d'approbation (au format XML) sont mis à jour. Nous étudierons plus loin le contenu de ces journaux.

MSUS offre des points de distribution multiples pour les patches Windows. Chaque serveur SUS peut servir jusqu'à 15000 clients (d'après Microsoft). Vous pouvez spécifier un ou plusieurs points d'approbation et de journalisation : il est possible de différentier chaque serveur MSUS parmi ces deux rôles, dans leur configuration, même si un seul serveur peut avoir les deux rôles simultanément.

La réplication entre les serveurs SUS internes est également basée sur les services « Automatic Updates » et BITS, permettant d'utiliser la bande passante non utilisée du réseau. Malgré ceci, le transfert des mises à jour peut être très long (parfois plusieurs jours !). Il faut en effet préciser qu'un jeu complet de patches pour un système tournant sous Windows 2000 / XP / 2003 représente actuellement environ 600 Mo par langue gérée (non compris Windows XP SP2, qui fait environ 270 Mo).

Le client MSUS est déjà présent dans Windows 2000 SP3 ou plus, Windows XP SP1 et Windows Server 2003. Pour les versions plus anciennes de Windows, il peut être téléchargé sous forme de setup depuis l'URL suivante :
http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp

Il remplace « Critical Update Notification » et précisons qu'il ne peut pas être désinstallé.

Le client est ses paramètres peuvent être déployés sur une station de travail en utilisant des GPOs ou des fichiers ADM (WUAU.ADM, disponible dans %WINDIR%\INF). Les paramètres sont stockés dans la clé de registre suivante :

HKLM\SOFTWARE\Policies\Microsoft \Windows\WindowsUpdate\AU.

Ces paramètres sont:

- L'adresse du serveur SUS (clé WUServer) ;
- Le planning de mise à jour (clés ScheduledInstallDay et ScheduledInstallTime) ;
- Les types de téléchargement et d'installation (clé AUOptions) : vous pouvez choisir d'effectuer une notification avant de télécharger le patch et/ou de le faire avant son installation ;
- Redémarrage automatique ou non (clé NoAutoRebootWithLoggedOnUsers). Si l'utilisateur connecté est Administrateur local, il a la possibilité de redémarrer immédiatement ou pas. S'il n'est pas Administrateur, le redémarrage est forcé. Vous pouvez aussi choisir de ne pas redémarrer automatiquement s'il y a des utilisateurs connectés et d'attendre le prochain redémarrage manuel.

Analyse des logs de MSUS

MSUS comprend 2 journaux d'activité : un journal de synchronisation et un journal d'approbation. Ils sont au format XML tous les deux. De plus, une journalisation de l'état des clients est également effectuée côté serveur : l'état des téléchargements et des installations de patches sont logués sur le serveur de statistiques. Comme noyus l'avons vu précédemment, le serveur de statistiques peut être différent du serveur SUS principal.

MSUS utilise les logs d'IIS pour écrire ses événements. Ces logs sont stockés dans les fichiers suivants :

```
%WINDOWS%/system32/LogFiles/W3SVCx/exyymmddhh.log
```

Cherchez `/wutrack.bin` dans ces fichiers pour trouver les lignes écrites par MSUS. Les statistiques de déploiement des patches peuvent être obtenues en analysant ces logs. Les entrées de MSUS dans les logs d'IIS sont de la forme :

```
/wutrack.bin?V=1&U=<Client_ID>&C=<client>&A=<activity>
&I=<item>&D=<device>&P=<platform>&L=<language>&S=<stat
us>&E=<error>&M=<message>&X=<proxy>
```

Exemple:

```
2004-08-16   16:09:55   127.0.0.1   GET   /wutrack.bin
V=1&U=cebed56691e3194998b908b01ddbbf7c&C=au&A=w&I=ie60
```

```
x.internetexplorer6x.ver_platform_win32_nt.5.2.x86.en.
..3790...com_microsoft.q824145_ie_server2003.&D=&P=5.2
.ece.2.112.3.0&L=en-US&S=f&E=80190193&M=ctx%3D5&X=
040108110352351 80 - 123.123.123.123 Industry+Update+
Control 200 0 0
```

Le champ « Client_ID » est un ID unique affecté à chaque ordinateur sur le réseau. Le champ « Status » indique l'état de l'installation du patch sur le client. Les valeurs possibles pour ce champ sont les suivantes :

- s – Succès
- r – Succès (redémarrage nécessaire)
- f – Echec
- c – Annulé (par l'utilisateur)
- d – Décliné (par l'utilisateur)
- n – Pas de patch (aucun correctif n'était disponible pour le système client)
- p – En attente

Vous pouvez utiliser l'outil « SUS Statistics Report tool » pour produire des rapports à partir des logs de MSUS. Cet outil gratuit peut être téléchargé à l'URL suivante :

http://www.susserver.com/Software/SUSreporting/

Cependant, il est recommandé de contrôler l'état des machines du réseau après chaque déploiement de correctif, à l'aide d'un scan MBSA (voir plus haut), et d'effectuer une analyse des logs MBSA pour détecter les ordinateurs sur lesquels les patches n'ont pas été appliqués avec succès.

Des logs sont également générés côté client pendant le processus de mise à jour. Ces logs indiquent si l'installation des patches s'est faite avec succès ou non. Ils sont contenus dans les fichiers suivants :

- `%programfiles%\WindowsUpdate\V4\IUHist.xml`
- `%windir%\Windows Update.log`

Trucs et astuces avec MSUS

Pour forcer immédiatement une détection et une mise à jour par le client AutoUpdate, suivez les étapes suivantes :

- Stoppez le service "Automatic Updates"
- Vérifiez que la valeur "AUState" dans la clé de Registry HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\ est à 2
- Détruisez la valeur "LastWaitTimeout" dans la clé de Registry HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\
- Démarrez le service "Automatic Updates".

Vous pouvez également approuver automatiquement les nouveaux correctifs, sans avoir à le faire manuellement dans l'interface Web d'administration de MSUS. En effet, SUS stocke sa base de données de correctifs dans des objets « dictionnaires » au format texte, situés dans le fichier suivant :

```
C:\InetPub\wwwroot\autoupdate\dictionaries\ApprovedItems.txt
```

Chaque correctif possède un enregistrement de la forme :

```
com_microsoft.q311889_xp_5081,1@|0@|0@|2003-08-01T15:06:35
```

Le premier "1" après la description indique l'état du correctif : 0= non approuvé, 1 = approuvé, 2 = nouveau, etc… Donc un simple rechercher/remplacer sur ce champ va mettre à jour la base de données de MSUS avec un nouvel état, remplaçant ainsi le processus manuel. MSUS va relire sa base de données la prochaine fois qu'il effectuera une synchronisation avec les serveurs de Microsoft, et considèrera donc les correctifs comme approuvés.

Vous pouvez trouver d'autres outils et scripts à l'URL suivante :

http://www.susserver.com/Tools/

Certains problèmes surviennent de manière récurrente : par exemple, les mêmes correctifs sont appliqués et réappliqués sans fin sur l'un des postes de travail. Dans ce cas, les critères de détection des correctifs peuvent être incorrects, ou la mise à jour échoue, ou encore l'installation réussit mais l'un des éléments de détection de mise à jour n'est pas correctement créé. Pour corriger cela, il est nécessaire de consulter la base de connaissance de Microsoft pour savoir quels sont les critères de détection et de faire les modifications nécessaires à la main, dans la Registry notamment.

Un autre problème provient du fait que certains correctifs et le patch cumulatif qui est censé les contenir sont appliqués un par un sur une machine. Malheureusement, MSUS 1.0 ne gère pas les patches cumulatifs. Il faut donc attendre la version 2.0 de MSUS et, en attendant, désapprouver les correctifs individuels inclus dans les patches cumulatifs suivants.

MSUS et SMS

MSUS peut s'intégrer à SMS 2.0 et SMS 2003 grâce au « SMS SUS Feature Pack », qui est gratuit et qui comprend plusieurs outils :

- Security Update Inventory Tool
- Microsoft Office Inventory Tool for Updates
- Distribute Software Updates Wizard
- Web Report Add-ins for Software Updates
- Elevated-rights Deployment Tool

Avec le SMS SUS Feature Pack, il est possible de déployer des patches pour toutes les plates-fomes et toutes les applications, et plus seulement les correctifs de sécurité de Windows. Il est également possible de suivre l'état des installations sur les clients : pour cela, l'outil mbsacli.exe est envoyé sur tous les clients pour effectuer un scan local (mbsacli.exe /hf), et le résultat est analysé pour savoir si l'application de certains correctifs a échoué.
Mais SMS est un produit coûteux, et les petites entreprises ne sont pas disposées à l'utiliser.

La version 2.0 de MSUS et les améliorations futures

MSUS 2.0 s'appellera Windows Update Services (WUS). Il devrait sortir à la fin de 2004 ou au début de 2005. Les principales améliorations apportées par cette nouvelle version seront les suivantes :

- Téléchargement des correctifs approuvés seulement (actuellement, tous les correctifs sont téléchargés depuis le site de Microsoft)
- Gestion des patches cumulatifs
- Désinstallation des patches désapprouvés
- Génération de rapports
- Gestion des autres applications Microsoft
- Unification de WindowsUpdate et OfficeUpdate en MicrosoftUpdate.

Microsoft a également décidé de diffuser les correctifs de sécurité « non urgents » une fois par mois (le deuxième mardi de chaque mois). Cela permettra aux administrateurs d'effectuer des cycles mensuels de tests et de diffusion des patches, afin que les correctifs individuels soient diffusés ensemble.

Les méthodes d'installation vont passer de 8 actuellement à 2 seulement : MSI 3.0 et UPDATE.EXE.
La taille des correctifs sera réduite. Aujourd'hui, la réduction de taille est d'hors et déjà de 35% environ. Avec WUS, cette réduction atteindra 80%, selon Microsoft. De plus, une technologie de « delta patching », déjà en fonction sur Windows Update, sera utilisée, et le processus sera amélioré avec MSI 3.0.

La durée d'indisponibilité sera réduite également. Actuellement, la diminution du nombre de redémarrages est déjà de 10% avec Windows 2000 / XP / 2003. Les redémarrages seront réduits de 30% avec Windows 2003 SP1 et jusqu'à 70% avec la prochaine version Serveur, selon Microsoft.

Après cette étude des outils de gestion des patches, nous allons maintenant voir comment une politique de gestion des correctifs de sécurité peut être implémentée dans le monde réel.

Mise en œuvre en grandeur réelle au sein d'un entreprise

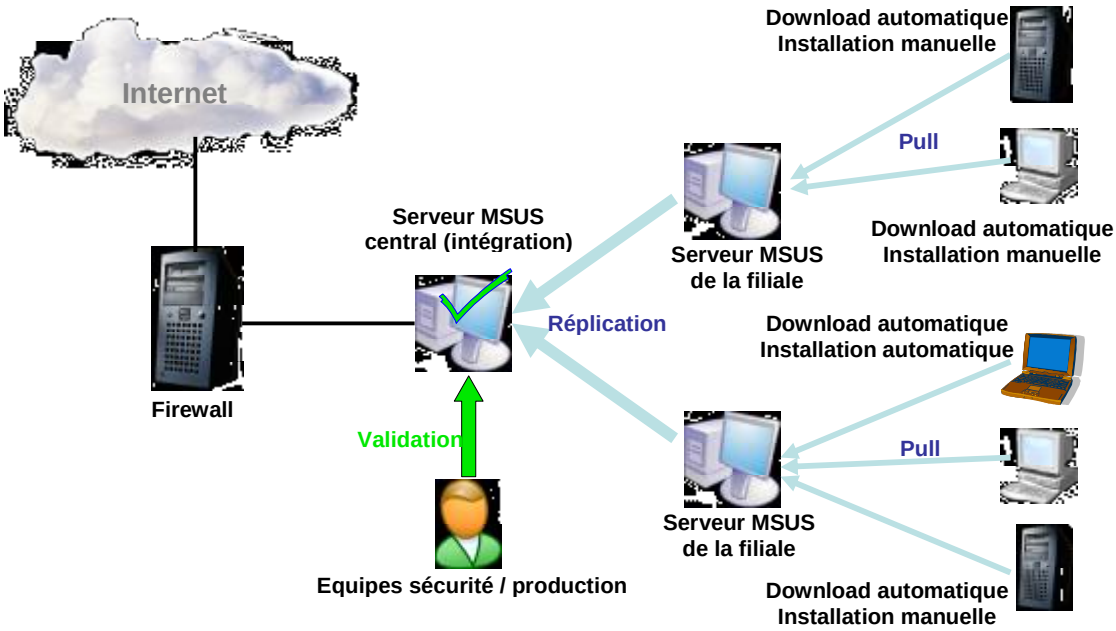
Accor Services est une Division d'Accor et le deuxième métier du Groupe après l'Hôtellerie. Avec une quarantaine de filiales dans 34 pays, Accor Services est le leader mondial du titre de services, avec comme produit phare le célèbre Ticket Restaurant®. Dans le cadre d'un projet de refonte et de centralisation de son SI, une politique de gestion de correctifs, basée sur des outils automatisés, a été définie et mise en place.

Cette politique se décline comme suit :

1. Une faille est publiée par un éditeur dont les produits sont utilisés au sein de l'entreprise (i.e. Microsoft), un patch y est généralement associé ;
2. L'équipe sécurité évalue le risque encouru (exploitabilité de la faille et impact potentiel) dans le cas particulier du SI de la société ;
3. Le correctif est testé sur une plate-forme dédiée ;
4. Un *advisory* interne est alors publié au sein de la Divison. Il traite notamment :
    a. des détails sur la faille découverte ;
    b. de l'existence ou non d'exploits[1] diffusés ;
    c. de l'existence ou non de scanners permettant d'identifier les machines vulnérables (ex. : eEye) ;
    d. des possibilités de contournements (*workarounds*) pouvant être mis en place, évitant ainsi d'appliquer un correctif sur un système dont l'indisponibilité serait préjudiciable ;
    e. des effets de bord éventuels du correctif (d'après les tests effectués et les informations extraites de la veille technologique interne).
5. Le correctif est alors mis en place sur un site d'intégration, reprenant l'ensemble des « serveurs d'infrastructure » (serveurs communs et génériques présents dans toutes les filiales déployées tels que les contrôleurs de domaine et serveurs de messagerie) ;
6. Après validation en intégration, le patch est téléchargé et installé automatiquement sur tous les PC (hors exceptions) ;
7. Concernant les serveurs, seul le téléchargement est automatique :
    a. L'installation se fait manuellement et à distance sur les serveurs d'infrastructure ;
    b. L'installation se fait manuellement et en local sur tous les autres serveurs et systèmes non mis à jour automatiquement (intervention des équipes informatiques locales).

Cette politique définit également la durée maximale de chacune des principales phases citées, de telle façon qu'un patch critique puisse être déployé en moins de 48 heures après validation (une semaine ouvrée pour les autres patches).

[1] Programme permettant d'exploiter une faille de sécurité au sein d'un applicatif, souvent la base d'un ver.



La mise en œuvre s'est faite grâce à MSUS. Un serveur central a été installé au Siège de la Division, tandis que des serveurs « esclaves » ont été mis en place dans chacun des sites déployés. Ainsi, lors de la validation d'un patch en central, les serveurs locaux viennent télécharger les correctifs avant de les diffuser sur les postes définis, à l'aide de GPO Windows (Group Policy Objects).

Depuis son implémentation avec MSUS, début 2004, cette politique a été enrichie et améliorée à plusieurs reprises. Les points à prendre en compte sont notamment :

- La programmation des téléchargements par zones géographiques, afin d'éviter la saturation du réseau lors des transferts de correctifs.
- Tenir compte des éventuels redémarrages après application des patches : en effet, certains correctifs nécessitent le reboot de la machine après leur application.
- Une politique spécifique doit être mise en place pour les postes nomades (de l'exclusion du réseau des postes non à jour au « patchage » automatique).
- Vérifier régulièrement le degré d'application des correctifs au sein du parc avec des scanners (MBSA notamment ou outils tiers) et l'éventuelle apparition de systèmes non à jour.

Conclusion

Comme nous l'avons expliqué plus haut, aucune Entreprise ne peut aujourd'hui s'affranchir de la mise en place d'une politique efficace de gestion des correctifs de sécurité. Si de nombreux outils existent (et nous n'avons pas détaillé les produits de télédistribution tels que SMS ou autres produits tiers), leur mise en œuvre nécessite une

véritable réflexion globale afin de limiter le temps d'exposition à une faille tout en ne pénalisant pas l'activité de l'entreprise.

Il faut noter que Microsoft semble œuvrer désormais de façon importante afin d'une part de rendre ses logiciels moins vulnérables (configuration par défaut plus restrictive pour Windows Server 2003 par exemple) ou exposés (firewall embarqué activé par défaut dans Windows XP SP2, protection de la mémoire contre les buffer overflows dans Windows 2003 et Windows XP SP2), tout en facilitant encore la gestion des correctifs (avec MSUS 2.0).

Ceci étant dit, de nouvelles formes de « hacking automatisé » risquent toujours d'apparaître un jour ou l'autre, rendant la veille plus que jamais indispensable à l'anticipation des problématiques de sécurité de demain.

Pour en savoir plus

- Méthodologie pour un processus de gestion des correctifs
  - http://www.giac.org/practical/GSEC/Daniel_Voldal_GSEC.pdf

- Microsoft Patch Management
  - http://www.microsoft.com/technet/security/topics/patch/

- MSUS:
  - Page principale
    - http://www.microsoft.com/windowsserversystem/sus/
  - MSUS Overview
    - http://go.microsoft.com/fwlink/?LinkId=6927
  - Articles et outils utiles
    - http://www.susserver.com/Tools/

- Configuration des mises à jour automatiques
  - http://support.microsoft.com/default.aspx?kbid=327838

- Microsoft Strategic Technology Protection Program
  - http://www.microsoft.com/security/mstpp.asp

- Security Operations Guide for Windows 2000 Server
  - http://www.microsoft.com/technet/security/prodtech/windows2000serv/staysecure/