MISC N° 22

Dossier : « superviser sa sécurité »

La gestion des correctifs de sécurité

Patrick CHAMBET
Architecte Sécurité du Système d'Information
Bouygues Telecom
http://www.chambet.com

La gestion des correctifs de sécurité, ou patch management, est aujourd'hui l'un des éléments clés de la protection des Systèmes d'Information. Il y a quelques années encore, la gestion des patches n'était nécessaire que sur un sous-ensemble relativement restreint de systèmes : principalement les serveurs les plus sensibles ou les plus exposés, comme les serveurs accessibles depuis Internet par exemple. Malheureusement, aujourd'hui, ce n'est plus aussi simple.

La cause principale est la diffusion récurrente de virus et autres vers auto-propagateurs. La menace a en effet évolué avec l'apparition de vers exploitant des failles de sécurité de logiciels largement répandus sur le marché, comme CodeRed, Nimda, Blaster, ZoTob, etc… Le périmètre vulnérable s'est par la même occasion considérablement élargi : il ne suffit plus de protéger les serveurs sensibles ou exposés, car toute machine (par exemple le PC bureautique d'un utilisateur) est une cible potentielle et peut se transformer à son tour en source de contamination. L'impact unitaire n'est, il est vrai, que de faible intensité, mais lorsque des milliers de PC sont infectés par des vers balayant des plages d'adresses entières à la recherche de machines vulnérables, c'est tout le réseau interne de l'entreprise qui peut être mis hors service pendant plusieurs jours, sans parler des éventuels effets de bord des vers ou virus en question (destruction de fichiers, diffusion à l'extérieur de documents confidentiels situés dans le répertoire « Mes Documents » ou sur le Bureau, 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 CodeRed à ZoTob 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 le cas du ver Witty, affectant les produits ISS, apparu dans la nature le lendemain de la publication officielle de la vulnérabilité qu'il exploitait !

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 dans le monde) s'accélère : quelques jours pour CodeRed, quelques minutes seulement pour SQL Slammer.

La gestion des correctifs de sécurité

Ainsi, il est nécessaire d'*agir* si l'on ne veut pas perdre son temps (et son argent) à *réagir* en cas de contamination : il s'agit d'être proactif plutôt que réactif. Cela n'empêche pas, bien sûr, de prévoir des processus d'urgence en réponse à la sortie d'un nouveau ver exploitant une vulnérabilité répandue ou d'un nouveau virus, d'où l'intérêt d'intégrer le processus de patch management dans son SOC (Security Operations Center) et dans sa supervision de la sécurité en général (voir les autres articles sur la supervision de la sécurité dans ce dossier).

La problématique de la gestion des correctifs de sécurité semble évidente au premier abord : il « suffit » d'installer régulièrement les patches diffusés par les éditeurs pour corriger les vulnérabilités de leurs systèmes d'exploitation, produits et applications. Cependant, dans la pratique, les entreprises se heurtent rapidement à de nombreuses difficultés, et celles-ci croissent de manière proportionnelle à la taille et à la complexité des Systèmes d'Information de l'entreprise : temps de réaction trop longs, multiplication des types de systèmes et des vulnérabilités associées, manque d'expertise technique, problèmes de régression, coûts de déploiement, gestion des matériels nomades, etc... Il est donc nécessaire d'industrialiser le processus de gestion des correctifs dans le contexte de son entreprise.

Une solution consiste à définir des stratégies de gestion proactives des correctifs, adaptées aux menaces et aux contraintes métier de l'entreprise, et à les implémenter à l'aide d'outils automatisés disponibles sur le marché. Nous allons donc, dans cet article, commencer par décrire différents types de stratégies de gestion des correctifs de sécurité, en se plaçant dans

l'hypothèse d'une grande entreprise, puis nous ferons un panorama rapide des outils de gestion des correctifs, en examinant plus en détail les outils fournis par Microsoft.

Les stratégies de gestion des correctifs de sécurité

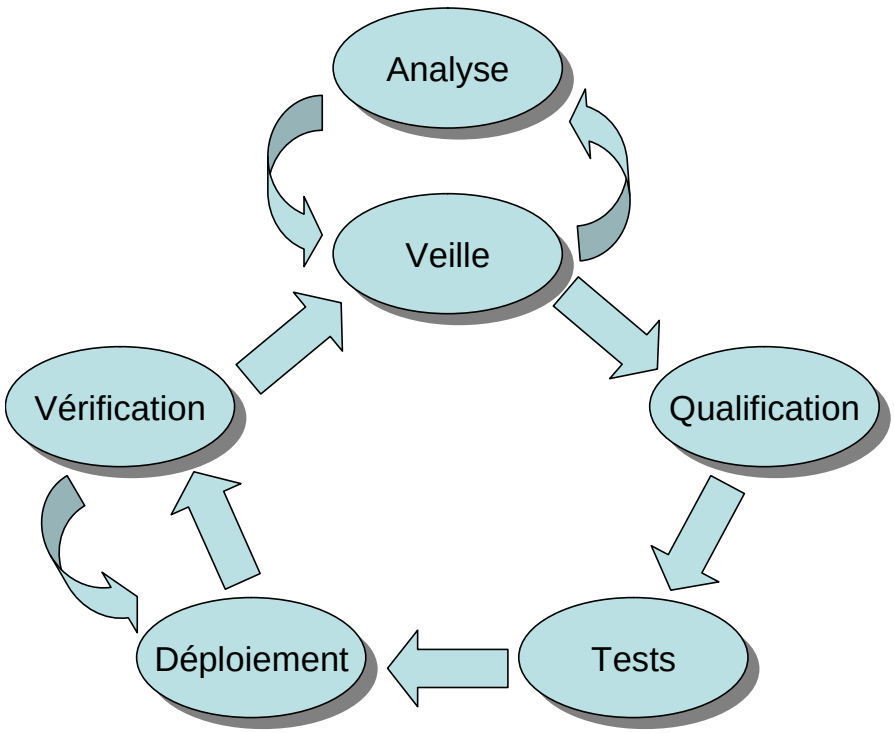
La problématique de la gestion des correctifs de sécurité dépend du contexte dans lequel on se place. En effet, la stratégie de patch management sera différente pour la production informatique et pour les postes bureautiques par exemple. De même, la stratégie d'application récurrente des patches sera différente de la gestion de crise utilisée en cas d'apparition d'une vulnérabilité critique ou d'un ver sur le réseau interne.

Dans les paragraphes suivants, nous allons commencer par analyser le processus habituel, récurrent, de la gestion des correctifs, en explicitant les différences induites par divers contextes d'exploitation.

Le processus récurrent

Nous nous plaçons ici dans un mode *proactif*. En effet, la plupart des éditeurs diffusent leurs correctifs à intervalle régulier, afin de permettre aux administrateurs d'effectuer des cycles de tests et de diffusion des patches, afin que les correctifs individuels soient diffusés ensemble. Microsoft diffuse par exemple ses correctifs de sécurité « non urgents » une fois par mois (le deuxième mardi de chaque mois), et Oracle publie ses correctifs majeurs tous les 3 mois (« Oracle Critical Patch Update »).

Le processus de gestion des correctifs est un processus itératif. Les étapes suivantes doivent en particulier être respectées :



Processus de gestion des correctifs

1 - Analyse

Il est nécessaire avant toute chose d'analyser l'existant dans l'entreprise, dans les différents types d'environnements (production, pré-production, intégration, bureautique, réseau, …) et d'effectuer une étude de risques mettant notamment en valeur les processus et les systèmes les plus critiques.

Un inventaire exhaustif du parc, y compris les ordinateurs portables (source majeure de problèmes dans bien des cas) permettra d'avoir toutes les informations nécessaires sur les types de systèmes et d'applicatifs, leur version, leur emplacement (DMZ ou cœur de production par exemple), etc… Un outil d'inventaire et de gestion de parc est le plus souvent indispensable pour recueillir ces informations et, surtout, pour maintenir leur cohérence dans le temps.

Il est également possible d'utiliser des scanners de vulnérabilités de type Nessus, bien qu'on commence à empiéter ici sur les étapes suivantes (voir article sur les VDS dans ce même numéro).

2 - Veille sécurité

Une fois l'inventaire matériel et logiciel établi, l'objectif de la veille sécurité est d'identifier les nouvelles vulnérabilités découvertes et/ou publiées concernant l'environnement existant, puis de trouver les mises à jour éventuelles mises à disposition par les éditeurs ou les fournisseurs, et ce, de manière fiable.

Cette veille sécurité peut être effectuée par l'équipe sécurité interne, par l'entité chargée de la gestion du parc informatique, ou encore être externalisée.

3 - Qualification

L'objectif de la qualification est, d'une part, de déterminer l'exploitabilité des vulnérabilités identifiées à l'étape précédente et leurs impacts potentiels, et, d'autre part, d'évaluer la pertinence de la diffusion des correctifs dans les différents environnements de l'entreprise et de définir si le processus à utiliser est le processus normal ou urgent.

Cette étape est donc primordiale : c'est à ce stade qu'il va être décidé si un correctif va être diffusé dans l'entreprise ou non, et si oui, dans quelles conditions et sur quel périmètre. En effet, le contexte du déploiement futur va influer à la fois sur l'évaluation de la criticité de la vulnérabilité et sur le coût de déploiement du correctif.

Prenons comme exemples les contextes de la bureautique et de la production.

Contexte de la bureautique

Le contexte de la bureautique est, d'une certaine manière, plus simple. En effet, les correctifs publiés par Microsoft sont à l'heure actuelle testés de manière extrêmement approfondie, et les effets de bord lors de leur déploiement sont de plus en plus rares. Un grand nombre d'entreprises a fait le choix d'appliquer les correctifs de sécurité diffusés par Microsoft (et surtout ceux qualifiés de critiques) sur l'ensemble de son parc Windows après un cycle de tests réduit, surtout en ce qui concerne les postes de travail. Dans la pratique, les problèmes de compatibilité avec les applications clientes installées sur les postes de travail sont très rares, et sont le plus souvent le fait de versions très anciennes de progiciels. En cas d'apparition d'un ver sur le réseau interne, tentant d'exploiter les vulnérabilités déjà patchées, le gain en fiabilité est évident.

Contexte de la production informatique

Dans un contexte de production, par contre, la qualification des correctifs doit être plus prudente et plus élaborée. Il n'est plus possible de déployer des correctifs sur des serveurs applicatifs sans

s'assurer au préalable que les impacts sur leur fonctionnement sont compatibles avec les contrats de service.

De plus, sur des parcs de très grande taille (plusieurs milliers de serveurs), il n'est souvent pas possible d'appliquer tous les correctifs diffusés par les éditeurs, pour deux raisons majeures :

- Appliquer tous les correctifs nécessiterait des arrêts et redémarrages permanents des systèmes en production ;
- Le coût du parc augmenterait de façon importante, sans apporter de gains suffisamment substantiels sur la fiabilité.

A cela s'ajoute la problématique des systèmes obsolètes, pour lesquels les éditeurs ne diffusent plus de correctifs de sécurité (Windows NT 4.0 par exemple). Cela peut survenir lors de la reprise de l'existant sur un parc de grande taille dont l'historique est conséquent, ou bien lorsque le parc contient des équipements de type « boîtes noires », contenant des éléments logiciels dont on ne maîtrise pas la nature (équipements Ericsson, par exemple). De plus, dans ce dernier cas, il est même interdit de mettre à jour les systèmes tournant dans ce type de solution packagée, sous peine de perdre la garantie de l'éditeur !

Pendant l'étape de qualification, qui est faite en général par l'équipe sécurité ou le bureau d'études interne, l'implication des maîtrises d'oeuvre des applications impactées est forte dans l'environnement de production : en effet, ce sont elles qui possèdent la connaissance des applications qui tournent sur les serveurs, et qui pourront donc qualifier les impacts applicatifs éventuels du correctif. C'est surtout le cas pour les progiciels (SAP, Siebel, …), un peu moins dans le cas de correctifs des OS sous-jacents.

Dans le cas d'Oracle, les impacts fonctionnels des patches peuvent être importants : en particulier, les correctifs Oracle, assez volumineux, requièrent souvent la mise en adéquation d'un grand nombre de dépendances. Ainsi, une mise à jour s'apparente plus à un projet de migration qu'à une simple mise à jour de sécurité. La validation par la maîtrise d'œuvre des applications est obligatoire dans ce cas.

4 - Tests

Une fois la qualification effectuée, il convient de tester l'application du correctif de sécurité sur un environnement suffisamment représentatif du périmètre cible. Pour les postes de travail, quelques postes installés avec les masters de l'entreprise, contenant les principales applications utilisées par les utilisateurs, seront suffisants.
Pour la production, on pourra bien sûr utiliser les environnements de tests applicatifs. Ensuite, une période d'observation sur un environnement de pré-production permettra de s'assurer de l'absence d'effets de bord ou de problèmes de régression.

Il ne faut pas oublier non plus de tester la désinstallation du correctif, au cas où un retour en arrière serait nécessaire plus tard.

5 - Planification et déploiement

C'est à cette étape que se prépare et s'exécute le déploiement et l'application des correctifs sur les systèmes cibles.

Les points à prendre en compte lors de la planification sont notamment les suivants :

- Programmer les téléchargements par zones géographiques, afin d'éviter la saturation du réseau lors des transferts de correctifs. Dans tous les cas, un contrôle de la bande passante doit être effectué.
- Certains correctifs doivent être appliqués dans un ordre précis.

- Tenir compte des éventuels redémarrages après application des patches : en effet, certains correctifs nécessitent le reboot des machines 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).
- Les créneaux de maintenance prévus sur les différentes cibles doivent être utilisés en priorité.

Sur un parc de grande taille, il est recommandé de s'appuyer sur un logiciel de déploiement durant cette étape, afin d'éviter que celle-ci s'étale sur une trop longue période, même en mode proactif. Les bons logiciels de gestion des correctifs comportent une fonctionnalité de hiérarchisation des correctifs selon le degré de criticité des vulnérabilités, et détectent les problèmes d'incompatibilité entre correctifs avant leur déploiement. De plus, certains outils, comme ceux de Shavlik par exemple, supportent des environnements hétérogènes. Nous étudierons dans le chapitre suivant quelques outils de gestion des correctifs.

Cependant, l'application des correctifs en mode manuel sur certaines machines est toujours possible, voire nécessaire, pour des serveurs situés dans certains types de DMZ, par exemple.
Dans tous les cas, le processus de déploiement doit être effectué en accord avec l'infogérant éventuel.

6 - Vérification

Cette étape finale consiste à vérifier que les correctifs ont été appliqués correctement sur tous les systèmes cibles. Pour cela, on peut utiliser les logs et les rapports générés par les outils de déploiement de patches (WSUS notamment, voir plus loin), ou utiliser des scanners de vulnérabilités (Nessus) ou de correctifs (MBSA 2.0 pour Windows par exemple).

Si des systèmes sur lesquels l'application des correctifs a échoué sont détectés, il convient alors d'en analyser la raison et de tenter un redéploiement de ces correctifs.

Cette vérification doit être effectuée régulièrement, afin de détecter l'éventuelle apparition de systèmes non à jour, par exemple.

Processus urgent

Le mode de déploiement urgent d'un correctif est un mode réactif utilisé lorsque, à l'étape de veille, un risque important est identifié. Il peut s'agir de la diffusion d'un ver sur le réseau interne, à partir du portable d'un prestataire par exemple (bien que la connexion d'un tel type de poste de travail doive être interdit). Cela peut aussi être le cas lorsque des serveurs accessibles depuis Internet sont vulnérables (exemple : vulnérabilité Apache, IIS, ou encore une vulnérabilité de la pile TCP/IP comme la vulnérabilité TCP CAN-2004-0230).

Dans ce cas, l'ensemble des étapes suivantes (qualification et tests en urgence, déploiement automatique ou manuel immédiat) doit être effectué en moins de 48h. De plus, dans le cas d'un ver, des mesures complémentaires de filtrage peuvent être prises, au niveau des firewalls, routeurs, firewalls personnels, etc…

Les outils de gestion des correctifs de sécurité

Nous avons vu que les approches classiques, basées sur des actions manuelles (`apt-get`) ou semi-automatiques (Microsoft Update, RHN) ne sont pas suffisantes à l'échelle d'une grande 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.

L'utilisation d'un outil de gestion des correctifs doit respecter un certain nombre de conditions, et notamment : qui ? quoi ? quand ? où ? et comment ?

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

Quoi : seules les mises à jour officielles des éditeurs devraient être appliquées. La vérification de leur origine est impérative. De plus, les administrateurs doivent tester et approuver les correctifs avant leur diffusion.
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 : on n'installera pas de patches Windows 2000 sur un système Windows XP, par exemple.

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 les périmètres qualifiés. 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.

Certains outils supportent en standard des plates-formes hétérogènes : PatchLink, par exemple, supporte Windows, Unix (Solaris, IBM AIX, et HP UX), Linux, Macintosh et NetWare. Certains nécessitent le déploiement d'un agent sur les machines, d'autres non. Les agents offrent souvent une plus grande richesse fonctionnelle (SMS par exemple) et consomment moins de bande passante, mais le coût de leur déploiement doit être évalué.

Environnements Microsoft

Microsoft propose plusieurs outils de gestion des correctifs :

- Scan des patches sur les machines : MBSA 2.0
- Mise à jour manuelle et semi-automatique : Microsoft Update
- Mise à jour automatique : WSUS (Windows Server Update Services) et SMS (Systems Management Server).

Nous allons étudier plus en détail ces outils dans les paragraphes qui suivent.

MBSA

MBSA 2.0 (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

MBSA 2.0 peut effectuer des scans en local ou à distance sur des systèmes Windows 2000 SP3 et plus, Windows XP, et Windows Server 2003. En plus des patches de sécurité Windows, il supporte également un grand nombre de produits Microsoft :

- Microsoft Office XP et plus
- Exchange Server 2000 et plus
- SQL Server 2000 et plus
- Et les autres produits supportés par Microsoft Update
  (voir : http://support.microsoft.com/?scid=kb;en-us;895660)

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\"
```

Fonctionnement de MBSA

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 personnel (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 WSUS 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*)

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.

Scripter MBSA

Les scans de MBSA peuvent être automatisés en utilisant des scripts : vous pouvez ainsi réaliser des tests à grande échelle. 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.

Microsoft Update

Microsoft 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://update.microsoft.com/microsoftupdate/, et un mode automatique ou semi-automatique, utilisant le service « Automatic updates » comme partie cliente. Microsoft Update est idéal pour les entreprises de petite taille.

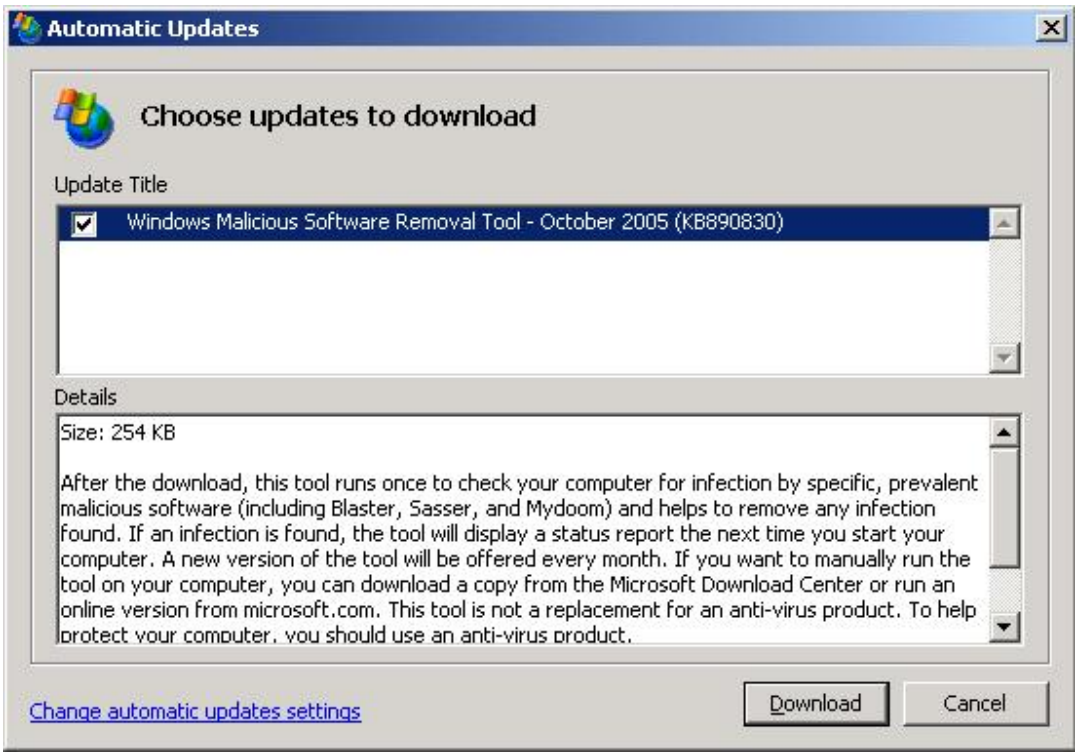
Lorsqu'il est utilisé en mode automatique, le service "Automatic Updates", qui permet une mise à jour automatique et en tâche de fond, nécessite que le service BITS (Background Intelligent Transfer Service) soit activé : ce service utilise la bande passante non exploitée afin de télécharger les patches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

Le client Microsoft Update 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 WSUS (voir ci-dessous).

Windows Server Update Services

WSUS est un outil gratuit qui peut être téléchargé à l'URL suivante :
http://www.microsoft.com/windowsserversystem/updateservices/downloads/WSUS.mspx

Contrairement à MSUS 1.0, qui ne gérait que les correctifs Windows, WSUS peut maintenant gérer les correctifs des produits suivants :

- Windows 2000 SP3+, XP et Server 2003
- Office (XP SP2 et 2003)
- SQL Server 2000
- Exchange Server 2003

Le principe de WSUS est d'avoir un serveur « Microsoft Update dans votre entreprise » : 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. Ceux-ci sont ensuite téléchargés sur les serveurs WSUS internes. Puis les postes utilisateurs se connectent automatiquement à l'un des serveurs internes de façon à télécharger et appliquer les patches validés.

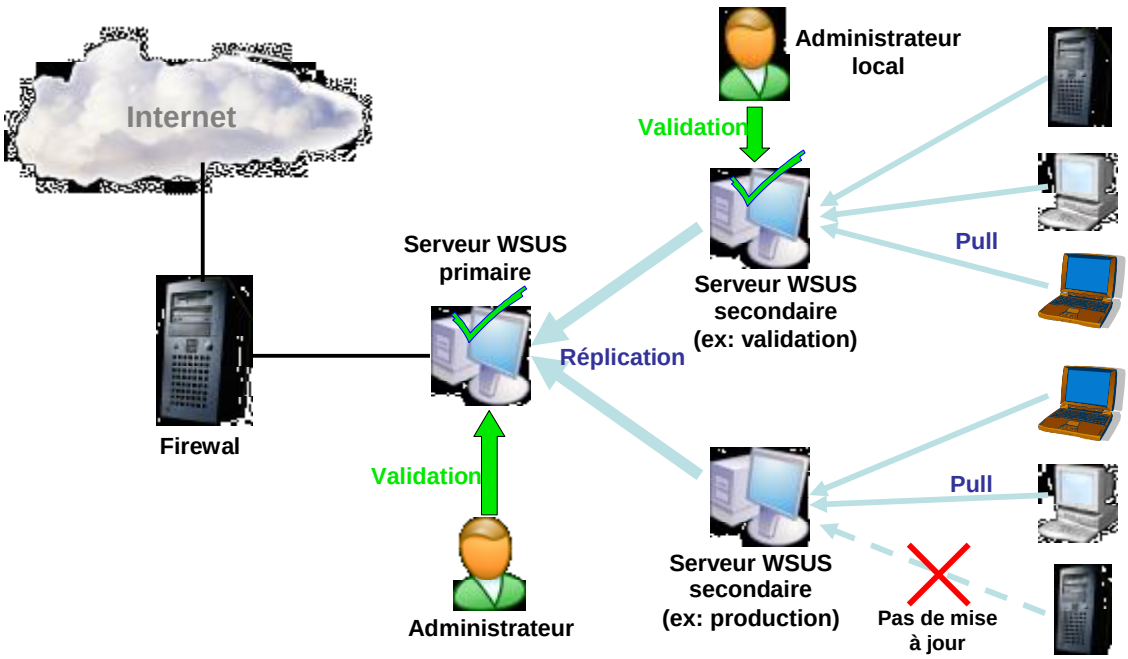
WSUS utilise une interface d'administration Web (http://wsus.votre-intranet.com/WSUSAdmin/) et a besoin d'IIS 6.0 sur les serveurs WSUS Windows Server 2003 internes.

Fonctionnement de WSUS

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

- WSUS télécharge un référentiel de sécurité (fichiers XML)
- Il valide la signature de Microsoft des CABs
- Il compare ce référentiel au contenu de sa base locale de façon à identifier les nouvelles mises à jour
- Il attend l'approbation de l'administrateur
- Il télécharge les patches approuvés par l'administrateur (uniquement) et vérifie leur signature
- Il met à jour ses journaux de synchronisation et d'approbation
- Si la synchronisation programmée échoue, WSUS réessaye trois fois avec à 30 minutes d'intervalle.

Une architecture WSUS avancée ressemble à ceci :



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

Qui : la partie cliente, 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 WSUS est installé sur votre réseau interne, il est recommandé d'interdire les domaines correspondant à Microsoft Update au niveau du proxy sortant afin qu'aucun utilisateur ne puisse mettre à jour une machine de sa propre initiative. Ces domaines sont notamment les suivants :

http://www.windowsupdate.com

http://windowsupdate.microsoft.com
http://update.microsoft.com

Quoi : Le serveur WSUS 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.).

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 WSUS. 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 WSUS.

Comment : les mises à jour sont d'abord approuvées par l'administrateur. Ensuite, les correctifs sont transférés entre le serveur WSUS principal et les serveurs WSUS 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, un unique redémarrage est effectué. Enfin, les journaux de synchronisation et d'approbation (au format XML) sont mis à jour.

WSUS offre des points de distribution multiples pour les patches Windows. La réplication entre les serveurs WSUS 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 1 Go par langue gérée.

Systems Management Server

SMS 2.0 et SMS 2003, qui sont destinés à l'origine à la gestion de parc (inventaire, télé-distribution d'applications, etc…) peuvent être utilisés seuls ou bien en combinaison avec des outils complémentaires proposés par Microsoft, spécialisés dans la distribution de correctifs de sécurité.

En effet, WSUS peut s'intégrer à SMS 2003 SP1 grâce à l'outil ITMU (Inventory Tool for Microsot Updates), qui est gratuit et permet de déterminer le niveau de patches des systèmes distants. Cet outil supporte les correctifs de Windows Update et Microsoft Update et est capable de les distribuer sur les systèmes qui le nécessitent (voir liens à la fin de cet article).

Par ailleurs, même sans ITMU, vous pouvez utiliser SMS 2.0 et SMS 2003 pour déployer des correctifs de sécurité, même si ce n'est pas l'objectif initial de SMS. Pour vous faciliter la vie, vous pouvez par exemple créer un paquet SMS « lanceur de correctifs intelligent » et ne nécessitant pas de recompilation à chaque ajout de correctif. Ajouter un correctif peut ainsi se réduire à compléter un fichier .INI décrivant ses prérequis, ses paramètres de ligne de commande et les informations de contrôle de bonne exécution.
De plus, dans un tel paquet SMS, vous pouvez en profiter pour inclure d'autres correctifs applicatifs, comme la mise à jour de l'anti-virus des postes de travail, par exemple.

Environnement Unix

Dans l'environnement Unix, chaque éditeur a développé ses propres mécanismes et ses propres outils de gestion des correctifs. De plus, de grands acteurs de la gestion de parc, comme Tivoli, BMC, Novell ou Computer Associates, mais aussi des spécialistes de la gestion de correctifs comme Criston, Landesk, Altiris, RippleTech, Ecora Software, Tenable, Shavlik, PatchLink et St Bernard Software, proposent des solutions intéressantes, car hétérogènes et intégrées.
Ces outils utilisent en général les mêmes principes que ceux présentés précédemment : analyse du niveau de patches, téléchargement des correctifs de sécurité, validation, distribution, vérification d'application correcte et enfin génération de rapports.

Voici un tableau de synthèse des outils (Unix, mais aussi Microsoft et Oracle) proposés par les éditeurs, le plus souvent gratuitement. Certains sont manuels (`apt-get`), d'autres automatisables (RHN par exemple) :

OS	Outils de scan des correctifs	Outils de gestion des correctifs
SUN Solaris	`pkginfo`	`patchadd`, `smpatch`, `install_cluster`, Sun Update Manager, Solaris Patch Manager, JumpStart
HP-UX	Security Patch Check Tool (`security_patch_check`)	Patch Assessment Tool, Custom Patch Manager
IBM AIX	`lslpp`	`instfix`, `installp`
Linux RedHat		`up2date`, `rpm` (RPM Package Manager), RHN (Red Hat Network)
Linux Debian		`dpkg`, `apt-get` (Advanced Package Tool)
Windows	MBSA 2.0	Microsoft Update, WSUS, SMS
Oracle		Patch Wizard, AutoPatch

Tableau de synthèse des outils de gestion de correctifs proposés par les éditeurs

Conclusion

Comme nous l'avons vu, 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, 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 les éditeurs semblent œuvrer désormais de façon importante afin de rendre leurs logiciels moins vulnérables (configuration par défaut plus restrictive des OS 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 WSUS notamment).

Cependant, de nouvelles formes de « hacking automatisé », toujours plus performantes, apparaissent régulièrement, 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

- Gestion des correctifs Microsoft
  - http://www.microsoft.com/france/securite/it/dossiers/correctifs/
  - http://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-chambet-larcher.pdf
  - http://www.chambet.com/publications/ISB-Patch_Management.pdf

- MBSA
  - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  - http://www.microsoft.com/technet/security/tools/mbsa2/qa.mspx

- WSUS
  - Page principale
    - § http://www.microsoft.com/windowsserversystem/updateservices/
    - § http://www.microsoft.com/windowsserversystem/updateservices/downloads/WSUS.mspx
  - WSUS Overview
    - § http://www.microsoft.com/windowsserversystem/updateservices/evaluation/overview.mspx
    - § http://www.microsoft.com/france/securite/evenements/journeesMicrosoftSecurite2005.mspx (2 présentations dans la page, en français)
  - Articles et outils utiles
    - § http://www.wsus.info
    - § http://www.susserver.com/Tools/
    - § http://www.wsuswiki.com

- SMS :
  - http://www.microsoft.com/smserver/default.mspx
  - ITMU : http://www.microsoft.com/smserver/downloads/2003/tools/msupdates.mspx

- MBSA 2.0 :
  - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  - http://www.microsoft.com/technet/security/tools/mbsa2/qa.mspx

- SUN :
  - Solaris Patch Management: Recommended Strategy : http://docs-pdf.sun.com/817-0574-12/817-0574-12.pdf http://www.sun.com/blueprints/0205/819-1002.pdf
  - Update Manager : http://docs.sun.com/source/835-0620/index.html
  - Patch Manager : http://www.sun.com/service/support/software/patchmanagement/patchmanager.html
  - http://sunsolve.sun.com/
  - http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches

- HP :
  - Patch Management User Guide for HP-UX : http://docs.hp.com/en/5991-1163/index.html
  - http://itrc.hp.com

- IBM :
  - http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html

    - http://techsupport.services.ibm.com/server/criticalfixes3/criticalfixes.html

- Linux RedHat :
    - http://www.redhat.com/software/rhn/
    - http://www.rpm.org/

- Linux Debian :
    - http://www.apt-get.org/

- Oracle :
    - http://www.oracle.com/technology/products/applications/upgrade_patching/