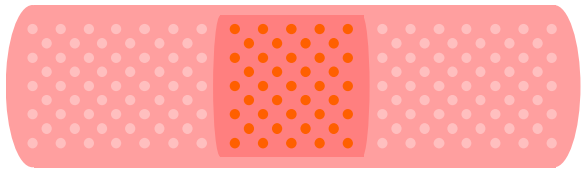
La gestion des correctifs de sécurité dans un parc Windows



Eric Larcher
Accor Services

info@internet-securise.com
http://www.internet-securise.com

Patrick Chambet
Edelweb

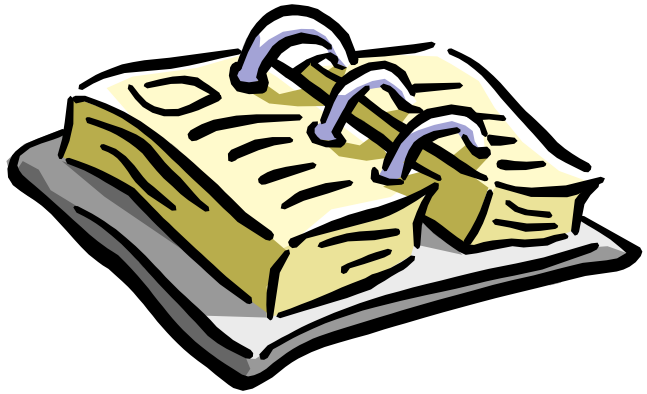
patrick.chambet@edelweb.fr
http://www.edelweb.fr
http://www.chambet.com

Objectifs

- Présenter les attaques récentes qu'ont subi les entreprises
- En déduire la nécessité d'une politique de mise à jour de l'ensemble d'un parc informatique
- Décrire certains outils de gestion des mises à jour de sécurité
- Présenter des éléments de politique de gestion des mises à jour à l'échelle d'une entreprise
- Conclure sur l'avenir des correctifs de sécurité

Planning

- Objectifs
- Généralités : quand les vers touchent le cœur des entreprises…
- Les outils de mise à jour
- Exemple de politique de mise à jour à l'échelle d'une entreprise
- Conclusion



Généralités (1/2)

- **Les intrusions ont pour causes principales**
  1. **Une mauvaise configuration d'un équipement**
  2. **Une vulnérabilité logicielle non corrigée**

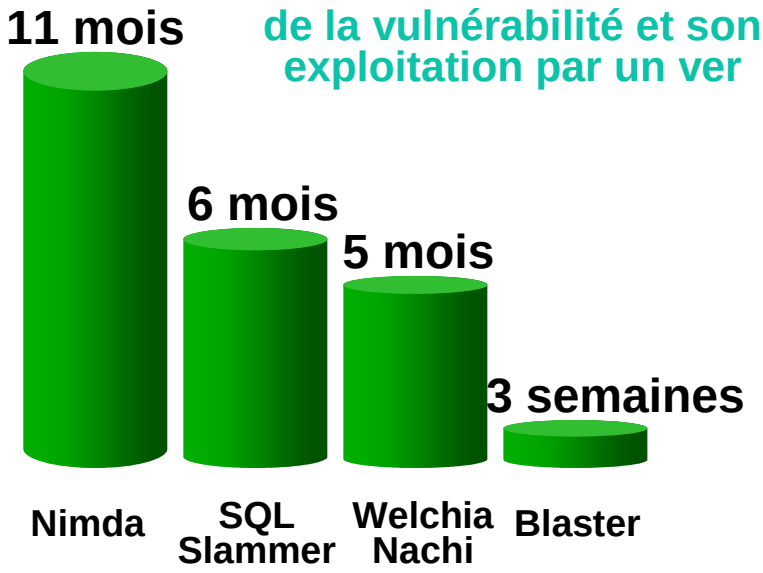
- **Les vers à propagation rapide utilisent la plupart du temps une vulnérabilité logicielle**
  - **CodeRed, Nimda, Blaster, …**

- **Autrefois, seuls les serveurs exposés nécessitaient une application rapide des correctifs**

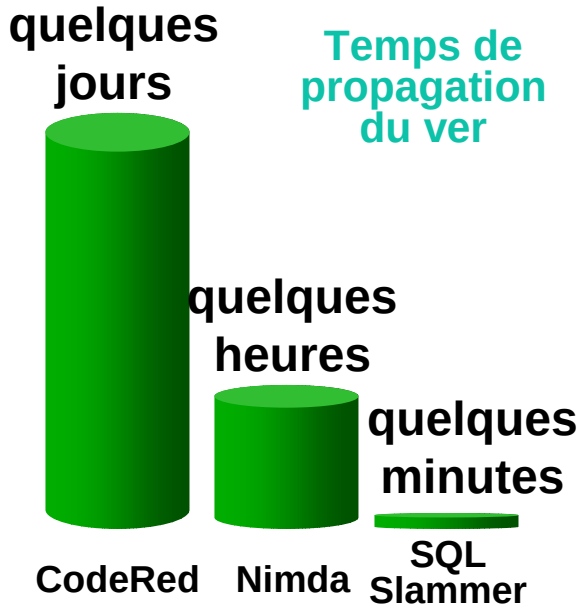
- **Actuellement, la prolifération des vers impose une mise à jour de la totalité des postes de travail en plus des serveurs**

Généralités (2/2)

- Exploitation des nouvelles vulnérabilités par les vers de plus en plus rapide

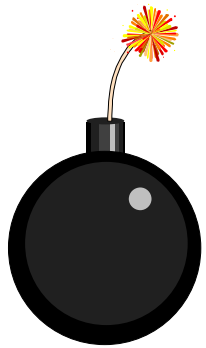


- Propagation des vers de plus en plus rapide



Scénario catastrophe

- Un ver pénètre le réseau interne de l'entreprise
  - Pièce attachée à un mail, serveur hostile, clé USB, ordinateur portable d'un commercial ou d'un prestataire externe, …



- Il se propage à tous les postes de travail et à tous les serveurs internes sur les réseaux non segmentés
- Il fait tomber certaines applications critiques, modifie aléatoirement le contenu de bases de données et fait sortir des informations confidentielles à l'extérieur de l'entreprise
- La reprise d'activité est impossible sans l'application préalable du correctif de sécurité correspondant sur toutes les machines, sinon réinfection immédiate

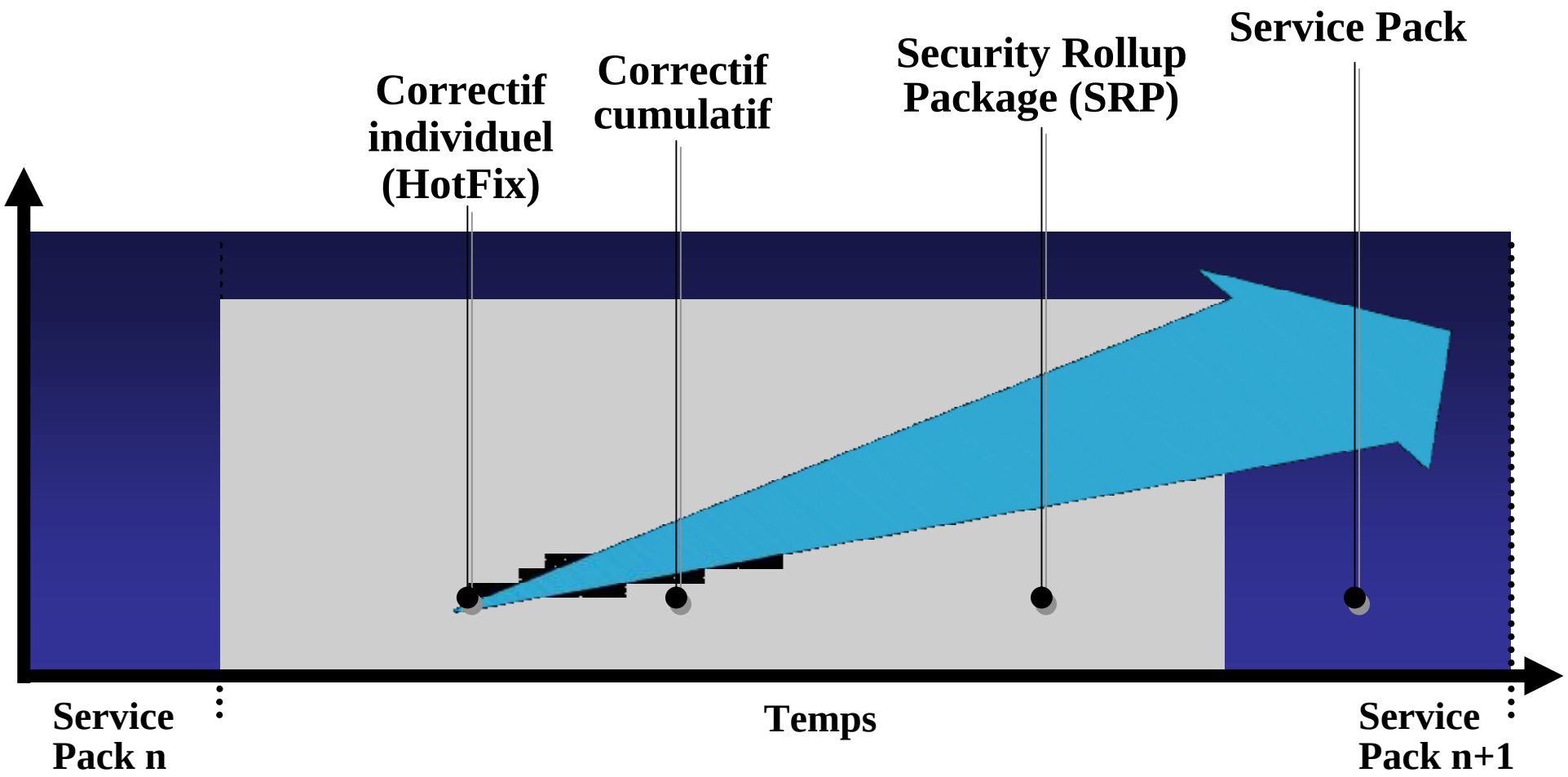
Constats

- La gestion des correctifs de sécurité est indispensable à l'échelle d'un parc

- Mais les approches actuelles ne sont plus suffisantes
  - Manuelles
  - Semi-automatiques (Windows Update)

- Intérêts de l'automatisation
  - Faciliter la veille des vulnérabilités et de leurs correctifs
  - Etre réactif face aux nouvelles menaces
  - Tester les correctifs avant de les déployer
  - Automatiser leur mise en oeuvre

Les différents types de correctifs Windows

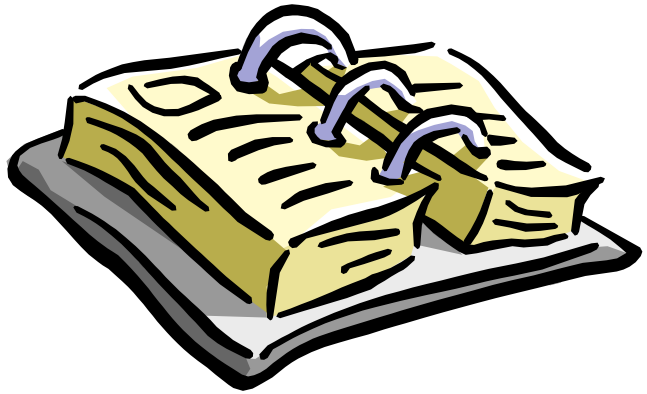


Problématique d'application des correctifs

- Qui ?
  - Les Administrateurs uniquement
  - Les utilisateurs ne peuvent appliquer de correctifs de sécurité
- Quoi ?
  - Correctifs de l'éditeur uniquement (vérification de la provenance)
  - Test et validation manuelle des correctifs par l'administrateur et rejet de ceux qui sont inutiles ou dangereux dans le contexte de l'entreprise
  - Sélection automatique des correctifs validés appropriés en fonction de la machine cible
- Quand ?
  - Automatiquement, avec planification
- Où ?
  - Sur chaque machine, y compris les portables itinérants (retour dans les locaux)
  - Depuis un ou plusieurs serveur(s) centralisé(s) de l'entreprise (le plus proche)
- Comment ?
  - Installation automatique en tâche de fond
  - Redémarrage unique, seulement si nécessaire (le moins possible)
  - Journalisation de l'issue de l'opération

Planning

- Objectifs
- Généralités : quand les vers touchent le cœur des entreprises…
- Les outils de mise à jour
- Exemple de politique de mise à jour à l'échelle d'une entreprise
- Conclusion



MBSA 1.1.1

- Microsoft Baseline Security Analyzer est une technologie Shavlik
- Outil graphique local
- Analyse la configuration de sécurité et détecte les erreurs de configuration de sécurité les plus courantes
- Télécharge un référentiel de sécurité XML, analyse le niveau de mise à jour par rapport à ce référentiel et détecte les correctifs de sécurité et Service Packs manquants
- Eléments supportés
  - Windows NT 4.0/2000/XP/2003
  - IIS 4.0 et 5.0
  - SQL Server 7/2000
  - IE 5.01+
  - Exchange 5.5 et 2000
  - Windows Media Player 6.4+
- Remplace HFNetChk
  - Ligne de commande: mbsacli.exe -hf -?

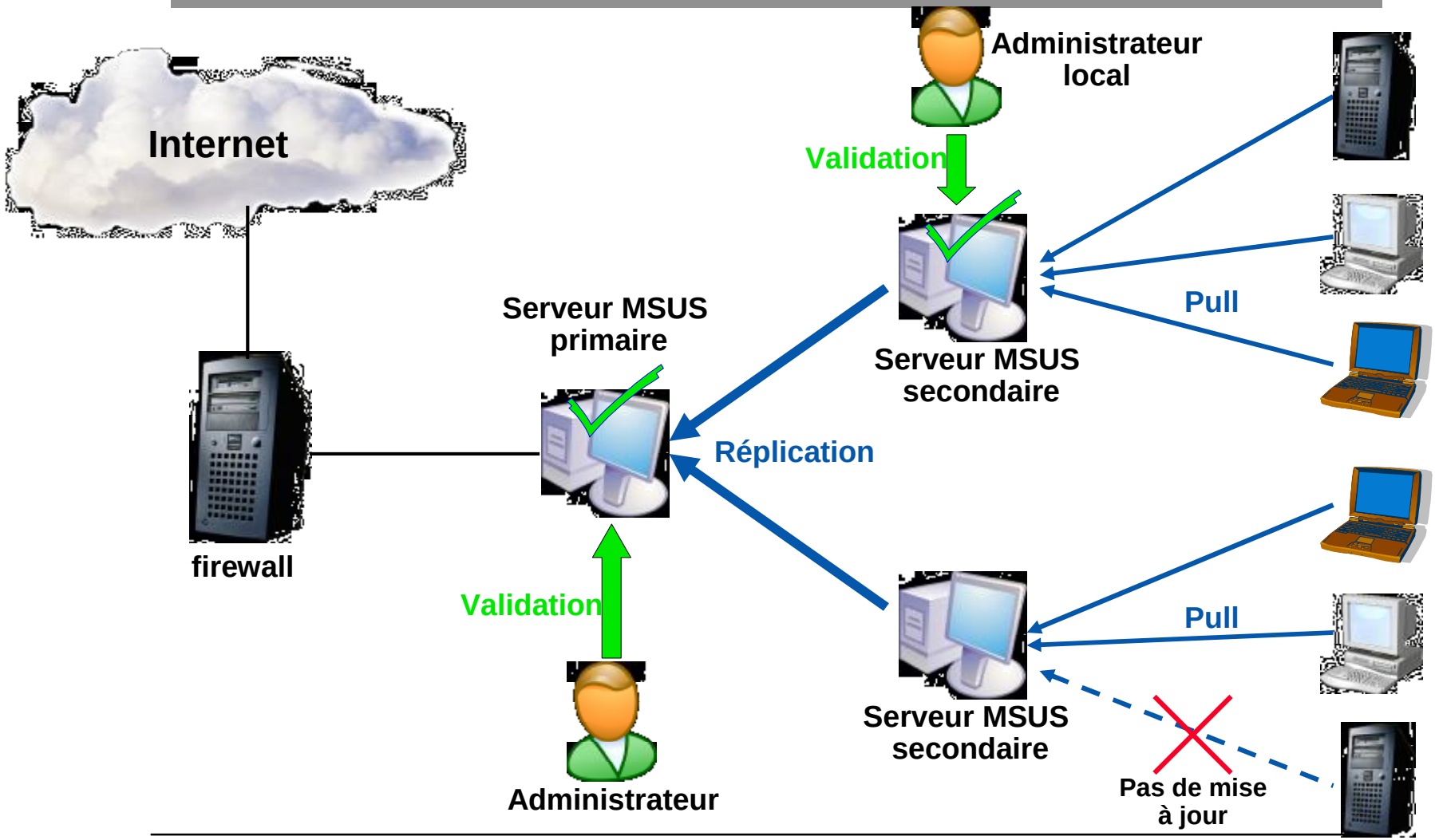
Windows Update

- Outil en ligne d'évaluation et de mise à jour de machines individuelles
  - http://windowsupdate.microsoft.com
- Client « Automatic Updates »
  - Service permettant la mise à jour automatique
  - Nécessite BITS (Background Intelligent Transfer Service)
- Vérifie que chaque correctif a été correctement installé
  - Clés de Registre
    - HKLM\SOFTWARE\Microsoft\Updates\Windows [VERSION]\SP[X]\
  - Liste des fichiers présents sur le disque
  - Version et hash de chaque fichier

MSUS

- Microsoft Software Update Service est un composant du programme STPP (Strategic Technology Protection Program)
- MSUS a été développé pour gérer les mises à jour de sécurité de Windows
  - Ne gère pas les applications
- Principe
  - Un serveur interne sur lequel se trouvent les mises à jour
  - L'administrateur approuve les correctifs nécessaires
  - Les clients se connectent sur le serveur pour installer les mises à jour approuvées
- Nécessite IIS pour fonctionner

Architecture MSUS



Déclinaison de la problématique avec MSUS 1.0 SP1 (1/2)

- **QUI**
  - Les Administrateurs des machines uniquement
  - Service « Automatic Updates » tournant sous le compte SYSTEM
  - Les utilisateurs ne peuvent appliquer les correctifs

- **QUOI**
  - Mises à jour pour Windows :
    - De sécurité (security updates)
    - De sécurité cumulatives (Security Rollup Packages)
    - Critiques (Windows critical updates)
    - Services Packs
  - Correctifs de Microsoft uniquement (vérification de la signature par le serveur)
  - Correctifs dans 31 langues
  - Sélection automatique des correctifs appropriés en fonction du poste client
  - Validation manuelle des correctifs et rejet de ceux qui sont inutiles ou dangereux

Déclinaison de la problématique avec MSUS 1.0 SP1 (2/2)

- **QUAND**
  - **Automatiquement (planification par heure +/- aléa)**
  - **Dès que le poste de travail démarre si l'heure est dépassée**

- **OU**
  - **Depuis chaque poste, en « pull » HTTP à partir du serveur SUS**

- **COMMENT**
  - **Contrôle administratif de l'approbation des mises à jour**
  - **Transfert en tâche de fond et optimisation de la bande passante (BITS)**
  - **Application automatique, en tâche de fond ou non**
  - **Redémarrage unique, seulement si nécessaire (30% du temps)**
  - **Journal de synchronisation et d'approbations (XML)**
    - **http://www.susserver.com/Software/SUSreporting/**

Publication interne

- Permet d'offrir des points de publication internes des correctifs Windows
  - Dimensionnés pour 15000 clients selon Microsoft
- Permet d'offrir un ou des points de validation et de journalisation
- Réplication entre serveurs SUS internes fondée sur les services « Automatic Updates » et BITS
- Utilise la bande passante non utilisée
  - Parfois très long
  - 550 Mo environ par langue gérée
- Paramétrage et déploiement sur les clients à l'aide de GPO
- Donne le choix ou non à l'utilisateur d'appliquer les patches s'il est administrateur

Déploiement

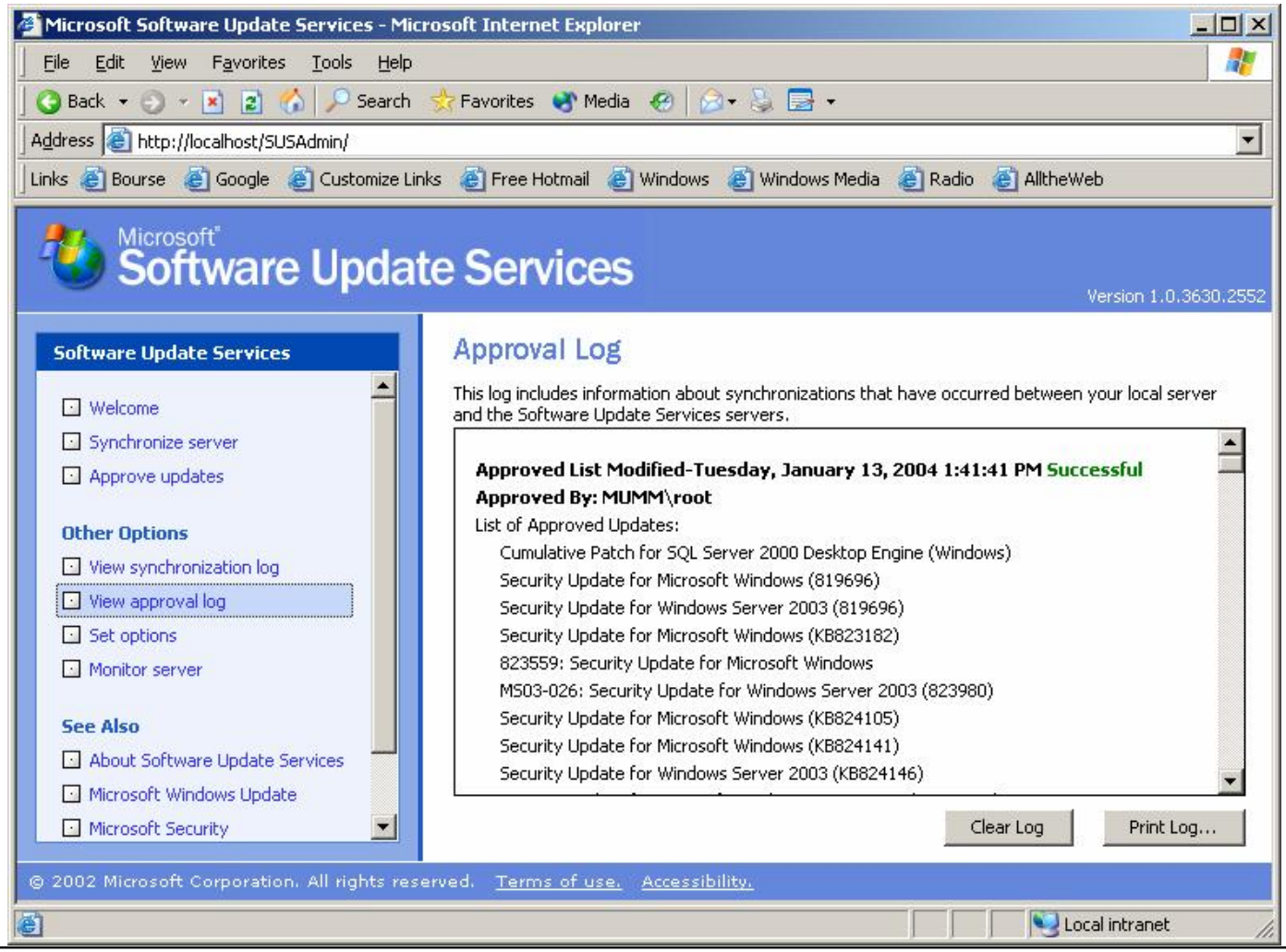
- **Client MSUS**
  - **Déjà intégré dans:**
    - **Windows 2000 SP3**
    - **Windows XP SP1**
    - **Windows Server 2003**
  - **Remplace « Critical Update Notification »**
  - **Ne peut être désinstallé !**
- **Fichier de stratégie ADM**
  - **Clé HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate**
    - **Adresse du serveur SUS**
    - **Type de download et d'installation**
    - **Redémarrage automatique ou non**
- **SMS SUS Feature Pack**
  - **Pour SMS 2.0 et SMS 2003**
  - **Gratuit**
  - **SMS 2003 permet en plus de déployer les correctifs pour toutes les plateformes et applications**

Configuration des accès sortants

- **Sites à autoriser pour le serveur MSUS principal**
  - **http://www.msus.windowsupdate.com**
  - **http://download.windowsupdate.com**
  - **http://cdm.microsoft.com**

- **Sites à interdire pour les autres machines (serveurs, postes de travail)**
  - **http://www.windowsupdate.com**
  - **http://windowsupdate.microsoft.com**

Administration



Administration

- Interface d'administration HTML
  - http://sus.intranet.fr/SUSAdmin
  - Installe IIS Lockdown et URL scanner sur le serveur IIS
  - Synchronisation du serveur
  - Approbation des correctifs
  - Paramétrage des options du serveur
  - Interface en anglais et japonais uniquement
- Suivi de l'activité
  - Journalisation dans les logs d'IIS
  - Statistiques de déploiement des mises à jour par analyse des logs d'IIS

Fonctionnement interne

- Téléchargement du référentiel de sécurité (base XML)
  - http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab
  - http://www.msus.windowsupdate.com/msus/v1/aurtf1.cab
- Validation de la signature
- Comparaison du référentiel pour déterminer les nouveaux correctifs
- Téléchargement des nouveaux correctifs et vérification de leurs signatures
- Mise à jour du journal de synchronisation et d'approbation
- Si la synchronisation planifiée ne fonctionne pas, SUS retentera la synchronisation 3 fois avec un intervalle de temps de 30 minutes

Amélioration de la gestion des correctifs (1/2)

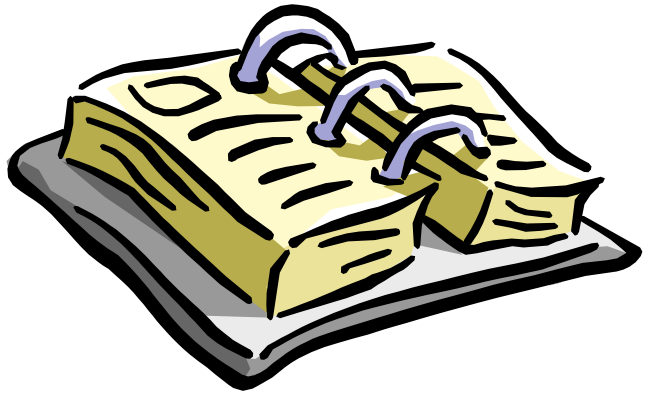
- Sortie de MSUS 2.0 début 2004
  - Téléchargement des correctifs approuvés uniquement
  - Gestion des correctifs cumulatifs
  - Désinstallation des correctifs désapprouvés
  - Génération de rapports
- Intégration des autres applications Microsoft (mai 2004)
  - Intégration de SQL Server et Exchange
  - Unification de WindowsUpdate et OfficeUpdate au sein de MicrosoftUpdate
- Extension du support sécurité jusqu'à juin 2004 pour
  - Windows 2000 SP2
  - Windows NT4 Workstation SP6a
- Publication mensuelle des correctifs de sécurité « non urgents »
  - Permet de planifier un cycle tests/déploiement de manière régulière
  - Fournis sous forme de correctifs individuels qui peuvent être déployés ensemble

Amélioration de la gestion des correctifs (2/2)

- Réduction du nombre de méthodes d'installation à 2 (au lieu de 8 actuellement)
  - MSI 3.0
  - UPDATE.EXE
- Réduction de la taille des correctifs
  - Actuellement : réduction de 35%
  - Mai 2004 : 80% de réduction (technologie de « delta patching », déjà en place sur WindowsUpdate, et amélioration des fonctionnalités avec MSI 3.0)
- Réduction de l'indisponibilité
  - Actuellement : 10% de réduction du nombre de redémarrages de Windows 2000/XP/2003
  - Mai 2004 : 30% de réduction pour Windows Server 2003 SP1
  - Jusqu'à 70% de réduction pour le prochain serveur selon Microsoft

Planning

- Objectifs
- Généralités : quand les vers touchent le cœur des entreprises…
- Les outils de mise à jour
- Exemple de politique de mise à jour à l'échelle d'une entreprise
- Conclusion



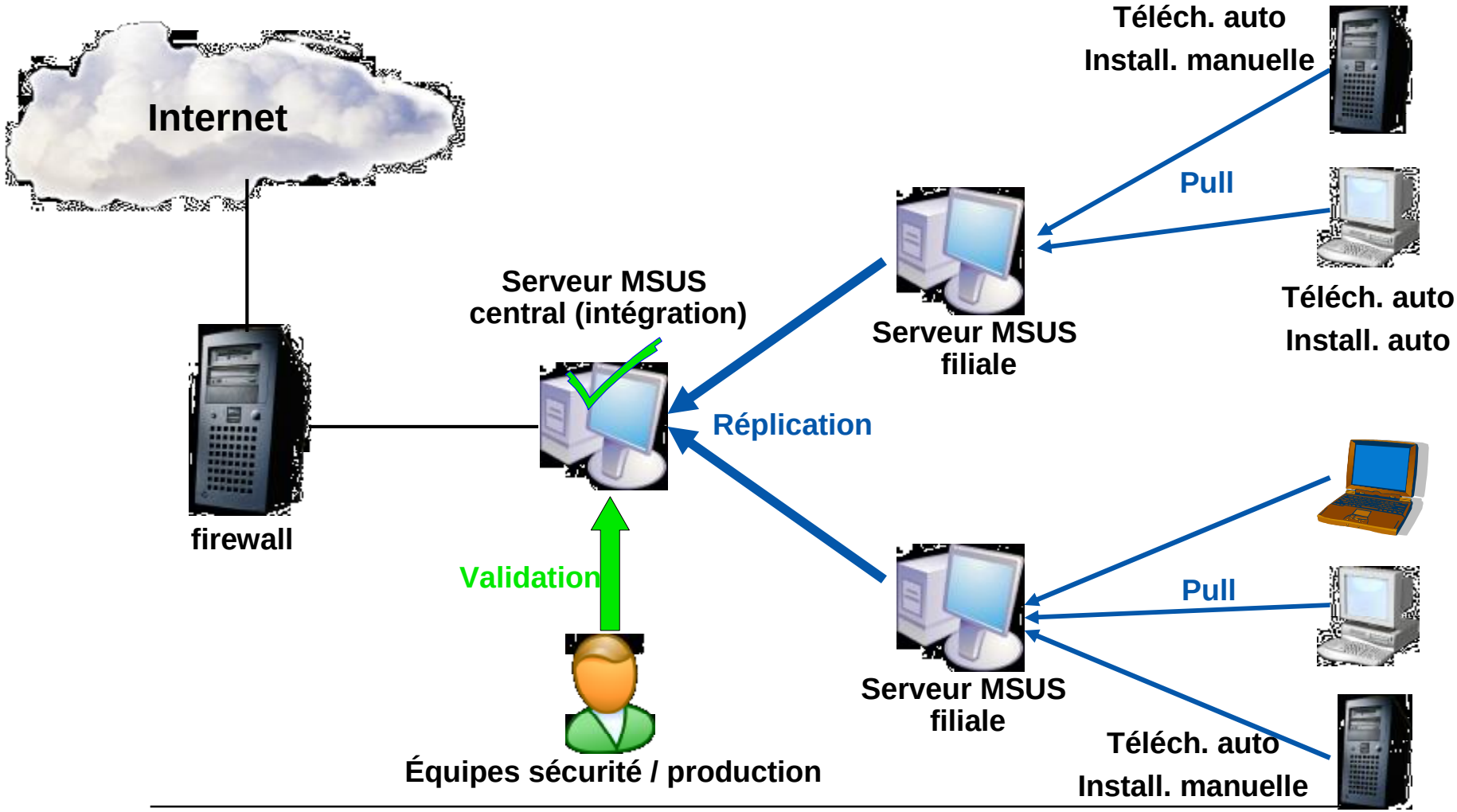
Exemple de politique (1/4)

- **Ancienne politique :**
  1. **Une faille est publiée, un patch sort**
  2. **Évaluation de sa pertinence et du risque encouru**
  3. **Test sur maquette dédiée**
  4. ***Advisory* interne à destination de toutes les filiales**
     - **Détails sur la faille corrigée**
     - **Existence ou non d'exploits diffusés**
     - **Disponibilité éventuelle de scanners (ex: eEye)**
     - **Possibilités de contournement (workarounds)**
     - **Effets de bord éventuels du correctif**
  5. **Application par chacune des DSI locales**
  6. **Si patch critique, suivi de son installation, filiale par filiale**

Exemple de politique (2/4)

- **Nouvelle politique :**
  1. **Une faille est publiée, un patch sort**
  2. **Évaluation de sa pertinence et du risque encouru**
  3. **Test sur maquette dédiée**
  4. ***Advisory* interne à destination de toutes les filiales**
     - **Détails sur la faille corrigée**
     - **Existence ou non d'exploits diffusés**
     - **Disponibilité éventuelle de scanners (ex: eEye)**
     - **Possibilités de contournement (workarounds)**
     - **Effets de bord éventuels du correctif**
  5. **Validation sur plate-forme d'intégration**
  6. **Téléchargement et installation automatiques sur les PC (hors exceptions)**
  7. **Téléchargement automatique sur les serveurs**
     - **Installation manuelle à distance sur les serveurs « d'infrastructure »**
     - **Installation manuelle en local pour les autres serveurs**

Exemple de politique (3/4)



Exemple de politique (4/4)

- Quelques remarques
  - Pour les entreprises mondiales, programmer les téléchargements par zones géographiques
  - Bien choisir son moment pour redémarrer les machines (serveurs, postes de travail)
  - Avertir éventuellement les utilisateurs par mail pour les patches critiques
  - Imposer la mise à jour des portables itinérants régulièrement (à travers leur accès VPN, sur le réseau local)
  - Contrôler l'état du parc après chaque déploiement
    - Scan avec HFNetChk ou MBSA
    - Traitement des logs de MBSA
    - Le journal de MBSA peut être exploité pour détecter les machines où l'application d'un patch a échoué

Conclusion

- Nécessité d'une politique de gestion des mises à jour de sécurité à l'échelle globale des entreprises
- Nécessité de rendre les logiciels plus résistants aux attaques, même quand les correctifs ne sont pas (encore) installés
  - Rôle de la configuration sécurisée par défaut => Windows 2003
- Intégration dans l'OS de technologies de protection
  - Firewall personnel (Windows XP/2003)
  - Protection de la mémoire contre les buffer overflows (.NET Framework)
- Technologies futures de sécurité au niveau de l'OS: TCPA/ NGSCB

Pour aller plus loin (1/2)

- 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/

Pour aller plus loin (2/2)

- 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/

Questions