Security Patches Management on a Windows Infrastructure

Patrick Chambet
EdelWeb – ON-X Group
patrick.chambet@edelweb.fr
http://www.edelweb.fr
http://www.chambet.com

Eric Larcher
Accor Services
info@internet-securise.com
http://www.internet-securise.com
Objectives

- Analyze some of the impacts of recent worm attacks against corporate networks
- Deduce from that the necessity of a security patches management policy for every computer on the network
- Describe some useful tools for security patches management
- Present some policies for patch management on a corporate scale
- Conclude on the security patches future
Planning

- Objectives

General points: when worms hit the heart of companies...

- Patch management tools

- Example of a typical policy for patch management on a corporate scale

- Conclusion
General Points

- Intrusions have some “root” ;-) causes
  1. A bad configuration of a system
  2. A non fixed software vulnerability

- Fast propagating worms use mostly a software vulnerability to infect a system
  - CodeRed, Nimda, Blaster, …

- Formerly, only Internet exposed servers needed hotfixing

- Today, spreading worms force admins to update every workstation on the network as well as servers
Worms Evolution

- The exploitation of new vulnerabilities by some worms is faster and faster

  - Time elapsed between the release of a new vulnerability and its exploitation by a worm:
    - Nimda: 11 months
    - SQL Slammer: 6 months
    - Welchia: 5 months
    - Blaster: 3 weeks
    - Witty: 1 day

- Faster and faster worm propagation

  - Propagation speed of the worm:
    - CodeRed: days
    - Nimda: hours
    - SQL Slammer: minutes
A relatively well secured enterprise with an antiviral policy is regularly infected by new virus and worms!
  - Don’t ask who… ;-) 

A “high skilled” consultant from a well-known consulting firm infected the whole network of a big company in France with his laptop
  - Don’t ask either…
Nightmare Scenario

◆ A worm penetrates the internal network of a company
  ➢ e-mail attachment, hostile Web server, USB key, laptop
  of a commercial person or an external worker, 1001 ways…!

◆ It propagates to every workstation and internal server
  on not segmented internal networks

◆ It crashes some critical applications, randomly
  modifies some database contents and leaks some
  confidential information outside of the company

◆ The recovery is impossible until the corresponding
  patch has been rolled out on every computer,
  otherwise the re-infection is immediate
Security patches management is essential on a corporate scale

But the current approaches are not enough

- Manual
- Semi-automatic (Windows Update)

Need for automation

- To facilitate the vulnerability and patch watch
- To be reactive to new threats
- To test patches before deployment
- To automate the roll-out
Typical Policy (1/2)

WHO?
- Administrators only
- Users mustn’t apply security patches

WHAT?
- Updates from the vendor only (verification of the origin)
- Test and approval of the patches by the Administrator and rejection of useless or dangerous ones (in the context of the company)
- Automatic selection of necessary patches (among approved ones), according to the nature of the target computer
Typical Policy (2/2)

◆ WHEN?
  - Automatically, with planning
  - MS recommendations
    - Critical patches within 24 hours, important patches within a month, moderate patches within 4 months and low-importance patches during the next 12 months

◆ WHERE?
  - On every computer, including mobile laptops (return to the office)
  - From one or more central corporate server(s) (the closest)

◆ HOW?
  - Automatic background installation
  - Unique reboot, only if necessary
  - Log events during and at the end of the operation
But Patches are not a Panacea...

I’m using nicotine patches to try to quit smoking. Yesterday, I experienced so much withdrawal symptoms that I rolled my patch and smoked it...

Marc Jolivet, French humorist
Planning

◆ Objectives

◆ General points: when worms hit the heart of companies...

✔ Patch management tools

◆ Example of a typical policy for patch management on a corporate scale

◆ Conclusion
Windows Security Patches

- HotFix
- Cumulative patch
- Security Rollup Package (SRP)
- Service Pack n
- Service Pack n+1
MBSA 1.2

- Microsoft Baseline Security Analyzer
  - Shavlik technology
  - Free version
  - Local or remote scans against Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 systems
  - GUI (mbsa.exe) or command line (mbsacli.exe) tool
    - Ex: to automate the tool
      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"
  - Replaces HFNetChk and MPSA
    - Command line: mbsacli.exe -hf -?

Patrick Chambet – Eric Larcher
Security patches management on a Windows infrastructure
MBSA 1.2

Supported products
- Windows NT 4.0, 2000, XP, 2003
- 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+
- Microsoft Office (local scans only)
- MDAC 2.5, 2.6, 2.7, and 2.8
- Microsoft Virtual Machine
- Commerce Server 2000, 2002
- Content Management Server 2001, 2002
- Host Integration Server 2000, 2004, and SNA Server 4.0
MBSA 1.2 Operation (1/2)

1. Analyses the security configuration
2. Detects the most common security configuration errors
   - File system
   - Admin accounts
   - Weak passwords
   - Running services
   - Shares
   - Audit policy
   - ICF configuration (local scan only)
   - Etc. (see the file: Checks.csv)
3. Downloads an XML security reference
   - From the Internet
     - http://go.microsoft.com/fwlink/?LinkId=18922
     - http://xml.shavlik.com/mssecure.cab (version 4.0)
     - http://xml.shavlik.com/mssecure.xml
   - From an internal MSUS server (scans for approved updates)
   - If MBSA cannot download mssecure.xml, it uses the local copy. So download Shavlik mssecure.xml and use it! (unsupported…)

4. Analyses the update level against the reference
5. Detects missing security patches and Service Packs
MBSA 1.2 Reference

◆ mssecure.xml

- Contains the security updates list since 1998
- For each patch are provided
  - Description
  - Download path
  - Path, version and checksum of files
  - Registry keys
- Updated every time a new security update is released
- Contains a history of previous hot fixes superceded by cumulative patches or SP
MBSA 1.2 Requirements (1/2)

- XML parser (MSXML 3.0 with latest SP)
- IIS common files (on the local computer to scan remote computers)

Ports

- TCP 80
  - To download mssecure.xml file
- TCP 139, 445
  - For remote computers scans

The user that launches MBSA must be a local Administrator
MBSA 1.2 Requirements (2/2)

**Required services**

- Computer being scanned locally
  - Workstation service
  - Server service

- Computer performing remote scans
  - Workstation service
  - Client for Microsoft Networks

- Computer being remotely scanned
  - Server service
  - Remote registry service
  - File and Print Sharing
MBSA Limitations (1/2)

- “Note messages” displayed for patches that can’t be confirmed
  - Products that don’t have detection
    - MSXML for MS02-008
  - More than one patch for a single product targeted at a particular OS (mssecure.xml schema limitation)
    - DirectX 9.0 for Windows 2000 / XP / 2003 (MS03-030):
      
```
Note MS03-030 Q819696
Please refer to http://hfnetchk.shavlik.com/support for a detailed explanation. Refer to the section on Note Messages.
```

- Sometimes can only check Registry keys to determine if a patch is installed
  - Ex: common Reg key for each Ntdll.dll version in MS03-007, but different file version and checksums

- When a non-security update overwrites files previously patched, MBSA reports the originally patched files as vulnerable

- Language of scanned computer determines if checksum checks are performed (/hf, /sum and /nosum options)
MBSA Limitations (2/2)

- **Registry key**
  Patch NOT Installed MS03-027 Q821557
  The registry key **SOFTWARE\Microsoft\Updates\Windows XP\SP2\KB821557\Type** does not exist. It is required for this patch to be considered installed.

- **File checksum**
  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].

- **File version**
  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].
Scripting with MBSA 1.2 (1)

- Scripts for automating MBSA scans
  - Enable large-scale scanning and enable low-rights end-users to check their own compliance without calling the helpdesk
  - `batchscan.js, rollup.js` scripts
    - Scan an unlimited number of computers or IP addresses from an input file
    - Compiles the results into a single summary report that can be viewed in Internet Explorer

- More info
### Scripting with MBSA 1.2 (2)

- Sample of single summary report
- XML file open in Internet Explorer

<table>
<thead>
<tr>
<th>Check</th>
<th>Critical</th>
<th>Warning</th>
<th>Passed</th>
<th>Note</th>
<th>Error</th>
<th>Informational</th>
<th>Not performed</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Version</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>296</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>317</td>
</tr>
<tr>
<td>File System</td>
<td>33 (10%)</td>
<td>0 (0%)</td>
<td>259 (82%)</td>
<td>0 (0%)</td>
<td>4 (1%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>317</td>
</tr>
<tr>
<td>Local Account Password Test</td>
<td>56 (18%)</td>
<td>12 (4%)</td>
<td>228 (72%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>317</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>0 (0%)</td>
<td>291 (92%)</td>
<td>4 (1%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>22 (7%)</td>
<td>317</td>
</tr>
<tr>
<td>Guest Account</td>
<td>10 (3%)</td>
<td>0 (0%)</td>
<td>282 (99%)</td>
<td>0 (0%)</td>
<td>4 (1%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>317</td>
</tr>
</tbody>
</table>
QChain (1/2)

❖ Command line tool to manually install several updates and reboot the computer only once

❖ Directions for use
  ➢ Launch updates with the “–z” option (no reboot)
  ➢ Launch qchain
  ➢ Reboot

❖ Unnecessary for Windows XP / 2003, that already includes a mechanism for simultaneous updates version management
  ➢ http://support.microsoft.com/support/kb/articles/Q296/8/61.asp
How to script patch installation

@echo off
setlocal
set PATHTOFIXES="C:\SUS\content\cabs"

%PATHTOFIXES%\Q123456_WXP_sp1_x86.exe -z -m
%PATHTOFIXES%\Q123321_WXP_sp1_x86.exe -z -m
%PATHTOFIXES%\Q123789_WXP_sp1_x86.exe -z -m
Etc...
%PATHTOFIXES%\qchain.exe result.log
shutdown.exe -t 60 -f
Windows Update (1/2)

Online patch checking and updating tool
- Manual
  - http://windowsupdate.microsoft.com
- Automatic
  - “Automatic Updates“ service
  - Ideal for small-sized companies

Automatic Updates client
- Service allowing an automatic and background update
- Requires the BITS service running (Background Intelligent Transfer Service)

Verifies that every patch has been correctly installed
- Registry keys
  - HKLM\SOFTWARE\Microsoft\Updates\Windows [VERSION]\SP[X]\KBxxxxxx
- File list on the disk
- Version and checksum of every file
Windows Update (2/2)

- Updates notification (for Administrators only)

![Windows Update Screen](image-url)
MSUS 1.0 SP1

- Microsoft Software Update Service
  - A component of Microsoft STPP program (Strategic Technology Protection Program)
  - http://www.microsoft.com/windowsserversystem/sus/default.mspx

- MSUS manages only Windows security updates
  - But we can see sometimes some exceptions...

- Does not manage applications (by now)

- Principle
  - One or more internal servers host the security updates
  - The administrator approves the necessary updates
  - Users connect to one of the internal servers to download and launch approved updates

- Requires IIS on the internal servers
- Unlike WindowsUpdate, MSUS doesn’t verify the serial numbers of the installed software... ;-)

Windows XP Driver 5.10.0.5410 for Realtek AC 97 Audio (KB833846), 4/9/2004
Download size: 3.6 MB
This is an update to the AC 97 audio driver on your system. Identified issues with the driver may cause your PC to stop responding. After you install this item, you may have to restart your computer. Once you have installed this item, it cannot be removed. Details...
Applies to: Windows XP Family
MSUS Internals

- Download of the security reference (XML files)

- Validation of the signature

- Comparison of the reference with the local database to determine the new updates

- Download of the new updates and verification of their signatures

- Update of the synchronization and approbation logs

- If the planned synchronization fails, SUS retries 3 times with a 30 min interval
MSUS Advanced Architecture

Primary MSUS server

Validation

Internet

Firewall

Local Administrator

Validation

Replication

Secondary MSUS server (ex: validation)

Pull

Secondary MSUS server (ex: production)

Pull

No update

Administrator
Policy Elements with MSUS (1)

WHO
- Computer Administrators only
- The « Automatic Updates » service runs with SYSTEM privileges
- Users cannot install updates

WHAT
- Windows patches only
  - Security updates
  - Security Rollup Packages
  - Windows critical updates
  - Services Packs
- Microsoft updates only (signature verification by the SUS server)
- Updates in 31 languages
- Automatic selection of appropriate updates (among approved ones), depending on each computer (OS version, language, …)
Policy Elements with MSUS (2)

◆ WHEN
  - Automatically (planning: specified time +/- random delay)
  - At boot time if the specified time is exceeded

◆ WHERE
  - On every computer
  - HTTP “pull” from the specified SUS internal server

◆ HOW
  - Test and approval of the updates by the Administrator
  - Background transfers and bandwidth optimization (BITS)
  - Automatic installation (background or not)
  - Unique reboot, only if necessary (30% of the time)
  - Synchronization and approbation logs (XML)
Internal Publication

- Offers multiple internal distribution points for Windows patches
  - Up to 15000 clients per SUS server (according to Microsoft)
- Offers one or more approval and logging points
- Replication between internal SUS servers based on « Automatic Updates » and BITS services
- Use of the unused bandwidth
  - Can be very long (sometimes several days !)
  - About 550 Mo per managed language
- If the user is a local Administrator, he has the choice to apply the patches or not
Deployment

◆ MSUS client
  - Already present in:
    - Windows 2000 SP3
    - Windows XP SP1
    - Windows Server 2003
  - Replaces « Critical Update Notification »
  - Cannot be uninstalled!

◆ Client and parameters deployment on workstations using GPOs or ADM files
Client Parameters

- Local GPO or WUAU.ADM installed in %WINDIR%\INF
- Registry key: HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
  - SUS server address
    - WUServer key
  - Update schedule (day and time)
    - ScheduledInstallDay key
    - ScheduledInstallTime key
  - Download and installation types
    - AUOptions key
    - Notify for download and / or notify for install
  - Automatic reboot or not
    - NoAutoRebootWithLoggedOnUsers key
    - No automatic restart with logged-on users
    - If the logged-on user is a local Admin, he has the choice
MSUS System Events

- Client side events can be collected
  - Unable to connect
  - Install ready – no recurring schedule
  - Install ready – recurring schedule
  - Install Success
  - Install Failure
  - Restart required – no recurring schedule
  - Restart required – recurring schedule
Outgoing Permissions

Sites to authorize for the primary SUS server
- http://www.msus.windowsupdate.com
- http://download.windowsupdate.com
- http://cdm.microsoft.com

Sites to forbid for other computers (servers and workstations)
- http://www.windowsupdate.com
- http://windowsupdate.microsoft.com
Administration

- Web based administration
  - http://sus.intranet.fr/SUSAdmin
  - Installs IISLockdown and URLScanner on the IIS server
  - HTTPS / SSL administration is possible
    - See Q326312
  - Server synchronization
  - Updates approbation
  - Set options
  - English and Japanese interfaces only
Approve Updates (1/2)

Choose the updates that you would like to distribute to your clients, and then click Approve.

- Security Update for Microsoft Data Access Components (KB823718), 1/12/2004 (New)
  - Download size: 1.6 MB
  - An identified security issue in Microsoft Data Access Components could allow an attacker to compromise a Microsoft Windows-based system and then take a variety of actions. For example, an attacker could execute code on the system. By installing this update, you can help protect your computer. After you install this item, you may have to restart your computer. Once you have installed this item, it cannot be removed. Details...
  - Applies to: Windows XP RTM, Windows XP SP1, Windows 2000 Family

- Security Update for Microsoft Data Access Components (KB832483), 1/12/2004 (New)
  - Download size: 2 MB
  - An identified security issue in Microsoft Data Access Components could allow an attacker to compromise a Windows-based system and take a variety of actions. For example, an attacker could execute code on the system. By installing this update, you help protect your computer. After you install this item, you may have to restart your computer. Once you have installed this item, it cannot be removed. Details...

Approved
Approve Updates (2/2)

- Status
  - New
  - Approved
  - Not approved
  - Updated : new version of an update, just downloaded
    - “Meta-patching” : patching of a patch 😊
  - Temporary unavailable
    - Unavailable associated update
    - Unfound dependency

- Note: an update that has already been applied and that is then labeled “non approved” will not be uninstalled by the AutoUpdate client
Multilingual Updates Mgt

◆ 31 languages supported

Language Settings
Choose the languages in which you would like the updates to be available.

- Arabic
- Arabic enabled
- Chinese Simplified
- Chinese Traditional
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Greek IBM
- Hebrew
- Hebrew enabled
- Hungarian
- Italian
- Japanese
- Japanese NEC
- Korean
- Norwegian
- Polish
- Portuguese (Brazilian)
- Portuguese (Standard)
- Russian
- Slovak
- Slovenian
- Spanish
- Swedish
- Thai enabled
- Turkish

OK  Cancel
MSUS Logs (1/2)

- **MSUS activity logs**
  - Synchronization and approbation logs (XML format)
- **Client status logging (server side)**
  - Downloads and installations status on the statistics server (can be different from the main SUS server)
  - Use of IIS logs to write events
    - `%WINDOWS%/system32/LogFiles/W3SVCx/exyy mmddhh.log`
  - Updates deployment statistics can be obtained by analyzing the logs (see after)
- **Client side logs**
  - Installation success and failure
    - `%programfiles%\WindowsUpdate\V4\IUHist.xml`
    - `%windir%\Windows Update.log`
MSUS Logs (2/2)

- The Automatic Updates client returns status on the following:
  - During Self-update: self-update pending
  - After Self-update: self-update success/failure
  - During Detection: initialization success/failure
  - After Detection: detection success, detection failure
  - After Download: download success/declined/failure
  - After Installation: installation success/declined/failure

- Note: nevertheless, it is recommended to control the state of computers on the network after every update deployment:
  - MBSA scan (see before)
  - MBSA log analysis to detect computers on which a patch hasn’t been applied successfully
MSUS Log Analysis (1/2)

- The status entries in IIS logs are in the following format
  - /wutrack.bin?U=<ping_ID>&C=<client>&A=<activity>&I=<item>&D=<device>&P=<platform>&L=<language>&S=<status>&E=<error>&M=<message>&X=<proxy>

- Example
  - 2004-01-08 16:09:55 127.0.0.1 GET /wutrack.bin
    V=1&U=cebed56691e3194998b908b01ddbbf7c&C=au&A=ie60x.internetexplorer6x.ver_platform_win32_nt.5.2.x86.en...3790...com_microsoft.q824145 ie_server2003.&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
MSUS Log Analysis (2/2)

- The “status” field indicates the status of the patch installation on the client
- Possible values are
  - “s” – Succeeded
  - “r” – Succeeded (reboot required)
  - “f” – Failed
  - “c” – Cancelled (by the user)
  - “d” – Declined (by the user)
  - “n” – No items (no update items were available for the client component)
  - “p” – Pending
- See SUS Statistics Report
Tips and Tricks (1/2)

How to force an immediate update detection of the AutoUpdate Client

1. Stop the "Automatic Updates" Service
2. Check that the "AUState" registry value in the HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\ key is set to 2
3. Delete the "LastWaitTimeout" registry value in the HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\ key
4. Start the "Automatic Updates" Service

More scripting tools

  - AUBehave.vbs: reads Automatic Update settings (in the Registry)
  - Autoapproveupdates.vbs: Auto Approve SUS patches (by messing with MSUS dictionaries)
  - SUS_Process_IIS6.vbs: SUS Log Reporting System (by analyzing IIS log files)
  - Etc...
How to automatically modify approved updates

- SUS stores its updates database in a dictionary object
  - `C:\InetPub\wwwroot\autoupdate\dictionaries\approvedupdates.txt`
- Each update has a record that looks like:
  - `com_microsoft.q311889_xp_5081,1@|0@|0@|2003-08-01T15:06:35`
- The first "1" after the description stands for the status of the update
  - 0 = unapproved, 1 = approved, 2 = new, etc...
- So a simple search and replace on this field updates MSUS database with new status information, bypassing the manual process
- SUS Service will then read and update this file when it next does a synchronization with the Windows Update servers
Troubleshooting

- The same updates are endlessly re-applied on a computer
  - Detection criteria are incorrect, or update installation fails, or the installation succeeds but one detection element isn’t recorded
  - See MS KB for detection criteria

- Some patches and related cumulative patches are installed one by one on a computer
  - MSUS 1.0 doesn’t manage cumulative patches.
    - When you approve a cumulative patch, un-approve individual patches embedded in the cumulative patch
MSUS Integration with SMS

- SMS SUS Feature Pack
  - For SMS 2.0 and SMS 2003
  - Free
  - Can deploy updates for every platform and application
  - Tracks the status of the client installations
    - Pushes mbsacli.exe to each client to perform local scan (mbsacli.exe /hf)
    - Parses output
MSUS Integration with SMS (2)

- SMS SUS Feature Pack includes the following tools
  - 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

- But SMS is expensive...
  - For big companies
Patch improvements (1/2)

- SUS 2.0 = Windows Update Services (WUS), release in S2 2004 (July ?)
  - Download of approved updates only
  - Management of cumulative patches
  - Uninstallation of un-approved patches
  - Report generation
  - Management of other Microsoft applications
  - Unification of WindowsUpdate and OfficeUpdate into MicrosoftUpdate

- Release of “non urgent” security patches each month (second Tuesday of the month)
  - Periodical test / roll-out cycles
  - Individual updates that can be deployed together
Patch improvements (2/2)

- Installation methods reduced from 8 (now) to 2
  - MSI 3.0
  - UPDATE.EXE

- Reduction of updates size
  - Today : reduction by 35%
  - S2 2004 : reduction by 80%
    - “delta patching” technology, already working on WindowsUpdate, and improvements with MSI 3.0

- Reduction of downtime
  - Today : reduction by 10% of reboots with Windows 2000 / XP / 2003
  - S2 2004 : reduction by 30% with Windows 2003 SP1
  - Up to 70% with the next Server, according to Microsoft
Planning

- Objectives

- General points: when worms hit the heart of companies...

- Patch management tools

Example of a typical policy for patch management on a corporate scale

- Conclusion
Policy Example (1/4)

- **Accor Services**
  - Presence in more than 34 countries, from Chile to Australia
  - More than 40 subsidiaries
  - Most subsidiaries have rather independent Information Systems

- **Our Goal: Patch Management in a Global Way**
  - Definition of a patch policy
  - A central security team watching for new vulnerabilities and patches
  - A new, centralized, information system being deployed worldwide
  - An automated update system for standard computers ("Infrastructure servers" and workstations)
Policy Example (2/4)

Accor Services Patch Policy

1. A vulnerability is discovered, a new patch is released

2. Evaluation of the scope of the vulnerability and the associate risk for the Company

3. Patch tests on a standard test lab
   - Windows
   - IIS / ASP
   - Exchange
   - SQL Server
   - Etc.
   - Use of VMWare or Virtual PC
Accor Services Patch Policy (continued)

4. Internal advisory published and sent to all subsidiaries
   - Information on the fixed flaw
   - Exploits availability
   - Vulnerability-specific scanners availability (ex.: eEye)
   - Possible workarounds description
   - Known side effects (detected during tests or reported in security newsletters)

5. Validation of the patch on the “infrastructure” test lab

6. Download and automated roll out on all PCs (except exceptions)

7. Automated download on all servers
   - Remote manual installation of “infrastructure” servers
   - Local manual installation for other servers
Policy Example (4/4)

Internet

Central MSUS server (integration)

Validation

Security / production teams

Auto download
Manual install

Auto download
Auto install

Auto download
Manual install

Firewall

Replication

Branch MSUS server

Pull

Branch MSUS server

Pull

Branch MSUS server

Pull
Problems & Advices

- Installation problems on few PCs
- Some systems sometimes can’t be patched (too old versions)
  - Ex.: at first, no RPC (MS03-039) patch available for NT4 Workstation and NT4 Server SP5
  - Some workarounds were found
- Not always easy to detect patch installation problems
  - MSUS logs show only patch executions, not patch failures
  - MS or other vendors’ scanners not always very reliable
- To reduce risks and improve performance, need to schedule patch distribution by geographic areas
- Use of VMWare or Virtual PC instances for patch testing (reduced number of test computers)
- Updates installation for remote users
  - They should use Windows Update
  - Possible to quarantine un-patched PCs (MS or third party tools)
Conclusion (1/2)

- A security patches management policy is mandatory on a global scale for companies

- Tools exist for all kinds of company size
  - Small size: automatic Windows Update
  - Medium size: MSUS
  - Big companies: MSUS or SMS + SUS Pack
Conclusion (2/2)

- Hardening software is essential, even when security patches are not applied (yet)
  - The default security configuration plays a crucial role => see Windows 2003

- Integration into the OS of protection technologies
  - Personal Firewall (Windows XP / 2003)
  - Memory protection against buffer overflows (Windows 2003)

- Future technologies at the OS level: TCP / NGSCB
Links (1/2)

- **Patch management**
  - Essentials and mailing list
    http://www.patchmanagement.org
  - Methodology
    http://www.giac.org/practical/GSEC/Daniel_Voldal_GSEC.pdf

- **Microsoft Patch Management**
  - FAQ

- **MSUS:**
  - Main Page
    http://www.microsoft.com/windowsserversystem/sus/
  - MSUS Overview
    http://go.microsoft.com/fwlink/?LinkId=6927
  - Useful articles and tools
    http://www.susserver.com/Tools/
Links (2/2)

- Automatic Updates configuration

- BITSAdmin tool:

- MBSA
  - Q&A

- Microsoft Strategic Technology Protection Program

Questions & Answers

Patrick Chambet – Eric Larcher
Security patches management on a Windows infrastructure