Implementing Security Update Management

Wayne Harris MCSE
Senior Consultant
Certified Security Solutions

Business Case for Update Management

When determining the potential financial impact of poor update management, consider:

- Downtime
- Remediation time
- Questionable data integrity
- Lost credibility
- Negative public relations
- Legal defenses
- Stolen intellectual property
Understanding the Vulnerability Timeline

Product shipped - Vulnerability discovered - Vulnerability disclosed - Update made available - Update deployed by customer

Most attacks occur here

Understanding the Exploit Time Line

Product shipped - Vulnerability discovered - Vulnerability disclosed - Update made available - Update deployed by customer

Most attacks occur here

<table>
<thead>
<tr>
<th>Malware Attack</th>
<th>Days between update and exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nimda</td>
<td>331</td>
</tr>
<tr>
<td>SQL Slammer</td>
<td>180</td>
</tr>
<tr>
<td>Welchia/Nachi</td>
<td>151</td>
</tr>
<tr>
<td>Blaster</td>
<td>25</td>
</tr>
<tr>
<td>Sasser</td>
<td>14</td>
</tr>
</tbody>
</table>

Days between update and exploit have decreased
Microsoft Update Severity Ratings

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Exploitation could allow the propagation of an Internet worm with user action</td>
</tr>
<tr>
<td>Important</td>
<td>Exploitation could result in compromise of user data or the availability of processing resources</td>
</tr>
<tr>
<td>Moderate</td>
<td>Exploitation is serious, but is mitigated to a significant degree by default configuration, auditing, need for user action, or difficulty of exploitation</td>
</tr>
<tr>
<td>Low</td>
<td>Exploitation is extremely difficult or impact is minimal</td>
</tr>
</tbody>
</table>

See “Microsoft Security Bulletin Search” on the Microsoft TechNet Web site

Update Time Frames

<table>
<thead>
<tr>
<th>Severity rating</th>
<th>Recommended update time frame</th>
<th>Recommended maximum update time frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Within 24 hours</td>
<td>Within two weeks</td>
</tr>
<tr>
<td>Important</td>
<td>Within one month</td>
<td>Within two months</td>
</tr>
<tr>
<td>Moderate</td>
<td>Depending on expected availability, wait for next service pack or update rollup that includes the update, or deploy the update within four months</td>
<td>Deploy the update within six months</td>
</tr>
<tr>
<td>Low</td>
<td>Depending on expected availability, wait for next service pack or update rollup that includes the update, or deploy the update within one year</td>
<td>Deploy the update within one year, or choose not to deploy at all</td>
</tr>
</tbody>
</table>
Improving the Updating Experience

<table>
<thead>
<tr>
<th>Your need</th>
<th>Microsoft response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce update frequency</td>
<td>Reduced frequency of non-emergency update releases from once per week to once per month</td>
</tr>
<tr>
<td>Reduce updating complexity</td>
<td>Reduced number of update installer technologies</td>
</tr>
<tr>
<td>Reduce risk of update deployment</td>
<td>Improved update quality and introduced update rollback capability</td>
</tr>
<tr>
<td>Reduce update size</td>
<td>Developed “delta updating” technology to reduce update size</td>
</tr>
<tr>
<td>Improve tool consistency</td>
<td>Developing consistent tools</td>
</tr>
<tr>
<td>Improve tool capabilities</td>
<td>Developing more capable tools</td>
</tr>
</tbody>
</table>

Defense in Depth

Using a layered approach:
- Increases an attacker’s risk of detection
- Reduces an attacker’s chance of success

ACLs, encryption, EFS
Application hardening, antivirus
OS hardening, authentication, patch management, HIDS
Network segments, IPSec, NIDS
Firewalls, Network Access
Quarantine Control
Guards, locks, tracking devices
Security documents, user education
Policies, Procedures, & Awareness
Requirements for Successful Update Management

Effective Processes
- People who understand their roles and responsibilities

Effective Operations
- Project management, four-phase update management process

Tools and Technologies
- Products, tools, automation

Update Management Process

Assess
- Inventory computing assets
- Assess threats and vulnerabilities
- Determine the best source for information about new updates
- Assess your software distribution infrastructure
- Assess operational effectiveness

Identify
- Discover new updates
- Determine whether updates are relevant to your environment
- Obtain update, confirm it is safe
- Determine if update is a normal change or an emergency

Deploy
- Prepare for deployment
- Deploy the update to targeted computers
- Review the deployment

Evaluate and Plan
- Determine whether the update is actually required
- Plan the release of the update
- Build the release
- Perform acceptance testing
Microsoft Update Management Guidance

- Guide: Patch Management Process
- How To: Implement Patch Management
- How To: Use Microsoft Baseline Security Analyzer (MBSA)
- How To: Perform Patch Management Using SMS
- Microsoft Server Windows Update Services Deployment Guide

The guide and articles are available on the Patch Management page of the Microsoft TechNet Web site.

The WSUS deployment guide is available on the Microsoft Windows Server Update Services Deployment Guide page of the Microsoft Windows Server System Web site.

Choosing an Update Management Solution

<table>
<thead>
<tr>
<th>Customer type</th>
<th>Scenario</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>All scenarios</td>
<td>Microsoft Update</td>
</tr>
<tr>
<td>Small organization</td>
<td>Has no Windows servers</td>
<td>Microsoft Update</td>
</tr>
<tr>
<td></td>
<td>Has one to three Windows 2000 or newer servers and one IT administrator</td>
<td>MBSA and WSUS</td>
</tr>
<tr>
<td>Medium-sized or large enterprise</td>
<td>Wants an update management solution with basic control to update Windows 2000 and newer versions of Windows</td>
<td>MBSA and WSUS</td>
</tr>
<tr>
<td></td>
<td>Wants a single flexible update management solution with extended level of control to update and distribute all software</td>
<td>Systems Management Server</td>
</tr>
</tbody>
</table>
Update Management Solution for Consumers and Small Organizations

- Update management solution based on Protect Your PC:
  1. Use an Internet firewall
  2. Get computer updates
     - Microsoft Update
  3. Use up-to-date antivirus software

- Deploy Windows XP SP 2
- See the Protect Your PC page on the Microsoft Security at Home Web site

Demonstration 1: Configuring Automatic Updates

Configuring Automatic Updates
Office Update

**Benefits:**
- Single location for office updates
- Easy to use
- Can download delta or full-file versions of updates

**Limitation:**
Does not support Automatic Updates; updating must be initiated manually

The Microsoft Update site includes Office updates and supports Automatic Updates.
Visit the Downloads page of the Microsoft Office Online Web site.

Update Management Solution for Small and Medium-Sized Organizations

<table>
<thead>
<tr>
<th>Size of organization</th>
<th>Scenario</th>
<th>Update management solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Has one to three servers running Windows 2000 or later and one IT administrator</td>
<td>MBSA and WSUS</td>
</tr>
<tr>
<td>Medium or large</td>
<td>Wants an update management solution with basic level of control that updates computers running Windows 2000, Windows XP, and Windows Server 2003 and some Microsoft applications</td>
<td>MBSA and WSUS</td>
</tr>
</tbody>
</table>
MBSA Benefits

- Scans systems for:
  - Missing security updates
  - Potential configuration issues
- Works with a broad range of Microsoft software
- Allows an administrator to centrally scan multiple computers simultaneously

MBSA is a free tool, and can be downloaded from the Microsoft Baseline Security Analyzer page on the Microsoft TechNet Web site

MBSA Considerations

MBSA reports important security issues:

- Password weaknesses
- Guest account not disabled
- Auditing not configured
- Unnecessary services installed
- IIS security issues
- Internet Explorer zone settings
- Automatic Updates configuration
- Windows XP firewall configuration
MBSA – How It Works

MBSA – Scan Options

MBSA has two scan options:

- MBSA graphical user interface (GUI)
- MBSA standard command-line interface (mbsacl.exe)

When scanning for security updates, you can configure MBSA to:

- Update the Microsoft Update Agent on all scanned computers
- Use a WSUS server as the update source
- Use Microsoft Update as the update source
Demonstration 2: Using the Microsoft Baseline Security Analyzer

- Scan a computer using MBSA
- Review an MBSA report
- Examine the Mbsacli.exe command-line tool

WSUS Benefits

- Gives administrators control over update management
  - Administrators can review, test, and approve updates before deployment
- Simplifies and automates key aspects of the update management process
  - Can be used with Group Policy, but Group Policy is not required to use WSUS
- Easy to implement
- Free tool from Microsoft
Comparing SUS and WSUS

**Common Features**
- Can only update computers running Windows XP, Windows 2000, or Windows Server 2003
- No option for pushing updates – clients must pull updates from the server

**WSUS Enhancements**
- Expanded support for Microsoft products such as Office, SQL Server, and Exchange Server
- Can create and manage computer groups
- More options for managing updates
- More options for configuring agents
- More efficient use of network bandwidth

WSUS – How It Works

- Microsoft Update
- WSUS Server
- WSUS Administrator
- Client Computers Group
- Pilot Computers Group
- Windows Servers Group
- Firewall
WSUS – Deployment Scenarios

WSUS – Client Component

The client component of WSUS is Automatic Updates

- Can be configured to pull updates either from corporate WSUS server or from Microsoft Update
- Three ways to configure Automatic Updates:
  - Centrally, by using Group Policy
  - Manually configure clients
  - Use scripts to configure clients
- WSUS requires a compatible Automatic Updates client
WSUS – Server Component

The server component of WSUS is Windows Server Update Services

- Can synchronize updates from Microsoft Update on a schedule
- Provides a Web-based administrative GUI
- Has several built-in default security features
- Provides synchronization and update reports
- Uses MSDE or SQL Server database to store update metadata, events, and settings
- Interface is localized in 17 languages

How to Use WSUS

On the WSUS server:

1. Administer the WSUS server at http://<server name>/WSUSAdmin
2. Configure the WSUS server synchronization schedule and settings
3. Create client computer groups and assign computers
4. Review, test, and approve updates

On each WSUS client:

Configure Automatic Updates on the client to use the WSUS server
Demonstration 3: Implementing Windows Server Update Services

- Configure Windows Server Update Services
- Configure Group Policy Settings for WSUS clients
- Distribute updates using WSUS
- View WSUS reports

Migrating from SUS to WSUS

To migrate from SUS to WSUS:
- You can install SUS and WSUS on the same computer
- You can migrate updates and approvals
- Use the WSUSUTIL.exe command-line tool
- Configure the clients to use the WSUS server
- Use the Automatic Update self-update feature to update the client
- For computers running Windows XP with no Service Packs, first install the SUS Automatic Update client
Update Management Solution for Medium-Sized and Large Organizations

<table>
<thead>
<tr>
<th>Capability</th>
<th>WSUS</th>
<th>SMS 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Platforms for Content</td>
<td>Windows 2000</td>
<td>Windows NT 4.0</td>
</tr>
<tr>
<td></td>
<td>Windows XP</td>
<td>Windows 98</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows XP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>Supported Content Types</td>
<td>Security and security rollup updates, critical updates, and service packs for the above operating systems and updates for some Microsoft applications</td>
<td>All updates, service packs, and updates for the above operating systems; supports updates and application installations for Microsoft and other applications</td>
</tr>
<tr>
<td>update Distribution Control</td>
<td>Basic</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

Systems Management Server Benefits

For a full software distribution update management solution, use:
- System Management Server 2003 or
- System Management Server 2.0 with SUS Feature Pack

Benefits of using System Management Server:
- Gives administrators comprehensive control over update management
- Automates key aspects of update management
- Can update a broad range of Microsoft products
- Can be used to update third-party software and install other software updates or applications
Systems Management Server – MBSA Integration

- MBSA integration included with SMS 2003 and the WSUS Feature Pack for SMS 2.0
- Scans SMS clients for missing security updates using mbsacli.exe /hf

1. SMS directs client to run local MBSA scan
2. Client performs scan, returns data to SMS server
3. SMS server parses data to determine which computers need which security updates
4. Administrator pushes missing updates only to clients that require them

Systems Management Server Considerations

Limitations of System Management Server:
- Command-line syntax must be configured for unattended installation of each update
- Microsoft Office updates require extraction to edit a settings file for unattended installation
- International updates must be manually downloaded from a Web page
Best Practices for Update Management

- Implement a good update management process
- Choose an update management solution that meets your organization's needs
- Subscribe to the Microsoft Security Notification Service
- Make use of Microsoft guidance and resources
- Keep your systems up to date
Session Summary

- Implementing security updates promptly is a critical component in a security management plan
- Update management needs to follow your standard network management processes
- For small and medium-sized business, MBSA and WSUS together provide an excellent update management solution

Next Steps

- Find additional security training events:
  - The Microsoft Security Events and Webcasts Web site
- Sign up for security communications:
  - The Microsoft TechNet Web site
- Order the Security Guidance Kit:
  - The Microsoft TechNet Web site
- Get additional security tools and content:
  - The Microsoft Security Web site