Updating and Patching using Microsoft Software Update Service
May 15, 2003
Jody Dunsworth
GSEC Version 1.4b Option 1

Abstract

Patch management is a requirement of the Windows operating system. The average Windows computer user not understanding this makes it difficult to keep a secure workstation environment. This paper will discuss a tool to help manage this problem, Microsoft's Software Update Service. "Microsoft Software Update Services (SUS) is designed to greatly simplify the process of keeping Windows-based systems up-to-date with the latest critical updates." [i] This software allows administrators to automate the download and install of software patches. The software will be discussed in general including how to install it, how to secure it, and the downside of it.

History

On January 25, 2003, Internet users noticed that traffic had slowed to a crawl. Upon further examination of the increasingly slow performance, it was discovered that an Internet worm, that would later be called the "Slammer worm," was infecting Microsoft SQL servers on the Internet. The worm spread across the entire planet in 12 minutes. Microsoft SQL Server had a flaw that had been discovered and a patch for this vulnerability was released approximately 100 days before this fast spreading worm began propagating. System administrators across the world were scrambling to install patches that had either never been installed or had been installed improperly. This is just one example of a time when malicious software had been written to exploit system flaws that had been known about and fixable for long periods of time.

Vulnerabilities are not limited to servers. In 2002 I received 10 Microsoft Security Bulletins dealing with only Microsoft Internet Explorer version 5.0 or newer. Of these 10, two were announcing security flaws that allow information disclosure. The other eight were reporting vulnerabilities that would allow an attacker to run the code of their choice on the compromised machine. These were only bulletins dealing with Internet Explorer; there were many others dealing with various other operating system components. During this time period a user running Internet Explorer would have had to install at least these 10 patches to ensure that these vulnerabilities were patched.

In my experience as a PC technician and Network Administrator I have found that many computer users have machines that are not running the most current software patches. Most people probably do not even realize that their computers need software patches. According to the SANS institute, failing to install security patches is ranked among the top 5 worst security mistakes made by end users.[ii] So why is it that we need to patch and update our software? Every day new exploits are announced revealing ways to compromise our computers. And why are the vulnerabilities not fixed before the product is released? Because the vulnerabilities are sometimes not discovered for several months to several years after the software is released. The code that makes up our operating system software today can be so complex that it is not possible to catch all of the possible security issues before it is released to the public. To remedy that, software makers release updated code to fix vulnerabilities that have been discovered. There are a number of ways that these patches can be applied to a system. Traditionally these patches have been manually downloaded and installed, but more efficient methods exist. There are a number of software packages to automate this process.

For a user to use the manual method of patch maintenance, they would need to search a website such as www.incidents.org or www.securityfocus.com for their operating system to determine any vulnerability. Then they would need to go to the software vendor's website to determine if there are patches available and if so, download and install them. This would require a considerable amount of knowledge, dedication, and time on a user's part, which would explain why most users have never patched their computer. In order to simplify this process Microsoft created windowsupdate.microsoft.com. This website allows a user to scan their computer and by comparing file versions can identify which patches their computer needs. This made the process much easier for the user, which increased the number of machines that were patched. Still, many users do not patch their computers because they do not understand what a software patch is and why patches need to be installed. Now there is a much easier way.

Introduction to Microsoft Software Update Service

Microsoft Software Update Service is a software package that allows system administrators to install software patches on computers connected to the network. Software Update Service (SUS) is installed on a server in a network environment and a client component (Automatic Update Client) is installed on workstations in the same environment. After configuration, the administrator will approve updates that will then be made available to the workstations. When a workstation checks the SUS server, it finds the updates and will install them. This removes the end user from the equation and ensures that the appropriate patches are installed in a timely manner, which provides for a more secure network.

Software Update Services consists of two equally important parts that the system administrator is responsible for. The first part is the Software Update

Server itself. This is the machine that will run the service for the network. The second part is the Automatic Update Client. This part resides on each client that needs to be included in the maintenance provided by this service.

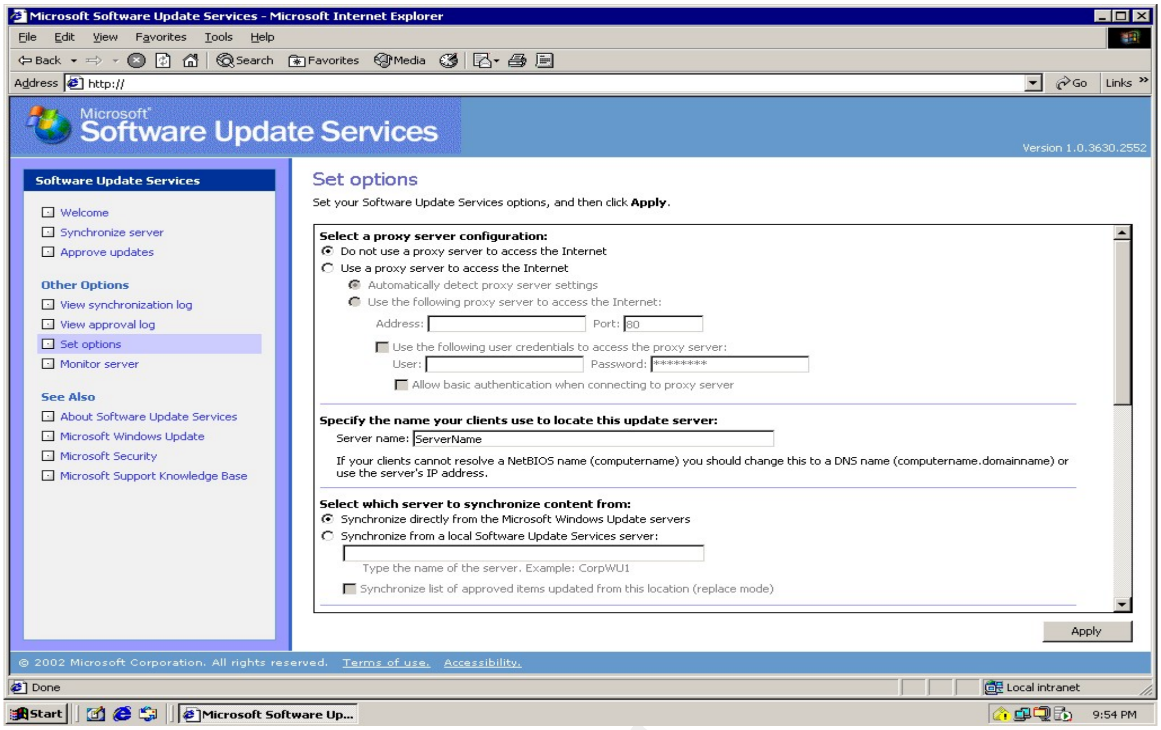
Installation

The Automatic Update Client has to be installed on all workstations that will be updated. There are several ways to install this on the workstations. The most basic is sitting at each machine and downloading it from Microsoft's website. For a small network with only a few machines this might be a good option, however for most networks this is not feasible due to the large number of machines that need the software installed. The easiest way to install the Automatic Update Client on a large network would be to push out the installer file (wuau22.msi) using Active Directory Group Policy Objects, Systems Management Server (SMS), or even a logon script. Another option is to install Windows 2000 Service Pack 3, Windows XP, or Windows 2003 Server. The most recent Automatic Update Client is included in each of these software packages. After the client has been installed, it must then be configured. This will be covered in a later section.

Next is the installation of Software Update Services on the server. The system requirements are:

- Pentium III 700 MHz or higher
- 512 Mb of RAM
- at least 6 Gb of free hard drive space
- Windows 2000 Server SP3, 2000 Advanced Server SP3, or Windows 2003 Server

After verifying that the hardware requirements are met, SUS can be downloaded directly from Microsoft at http://go.microsoft.com/fwlink/?LinkId=6930. To minimize the chance of downloading and installing a trojanized version I would recommend downloading directly from Microsoft and not from a third party website. (Unfortunately, Microsoft does not currently provide any type of signed checksum verification on the download to ensure that we have a valid file.) After downloading, the file should be placed on the server where it will be installed. After installing, it should be configured using the admin webpage that is setup during the install. The path to this page will be http://servername/SUSAdmin. This page will allow customization of the service, such as when and how the server synchronizes content from Microsoft. Also the setup page allows for the use of a proxy server for the connection to the Windows Update Servers.



Microsoft Software Update Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://
Go Links

Microsoft® Software Update Services

Version 1.0.3630.2552

Set options

Set your Software Update Services options, and then click **Apply**.

Select a proxy server configuration:

● Do not use a proxy server to access the Internet
○ Use a proxy server to access the Internet
● Automatically detect proxy server settings
○ Use the following proxy server to access the Internet:
Address: Port: 80
□ Use the following user credentials to access the proxy server:
User: Password: *********
□ Allow basic authentication when connecting to proxy server

Specify the name your clients use to locate this update server:

Server name: ServerName

If your clients cannot resolve a NetBIOS name (computername) you should change this to a DNS name (computername.domainname) or use the server's IP address.

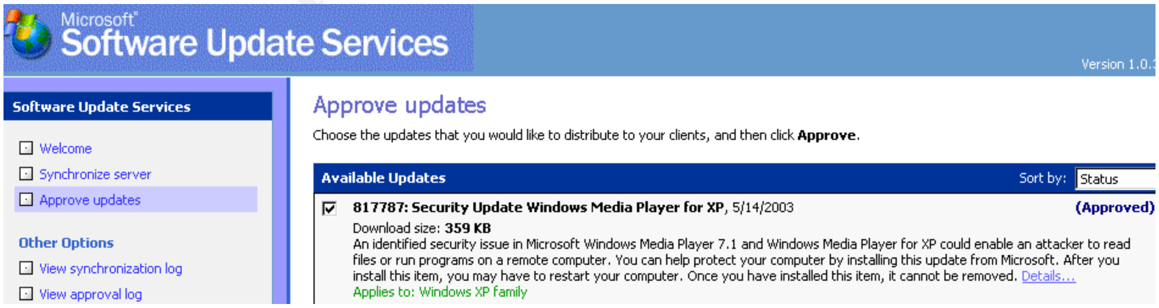
Select which server to synchronize content from:

● Synchronize directly from the Microsoft Windows Update servers
○ Synchronize from a local Software Update Services server:
Type the name of the server. Example: CorpWU1
□ Synchronize list of approved items updated from this location (replace mode)

Apply
© 2002 Microsoft Corporation. All rights reserved. Terms of use. Accessibility.
Done
Local intranet
Start
Microsoft Software Up...
9:54 PM

Server Configuration

After setting the server name, location to synchronize the updates from, and the proxy information, the next step is to setup the synchronization schedule. Software Update Services provides the option to only synchronize manually or to choose a time and day or days to automatically retrieve the updates. After synchronizing the server, the administrator can then view the list of updates available for installation. This list gives the administrator the opportunity to install the same updates on test machines to verify that they will not cause any problems after installing.



Microsoft® Software Update Services

Version 1.0.

Approve updates

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

Available Updates Sort by: Status

☑ **817787: Security Update Windows Media Player for XP**, 5/14/2003 **(Approved)**
Download size: **359 KB**
An identified security issue in Microsoft Windows Media Player 7.1 and Windows Media Player for XP could enable an attacker to read files or run programs on a remote computer. You can help protect your computer by installing this update from Microsoft. 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

To test the updates we click on the “Approve updates” link, which will show the list of available updates to approve. Then click on the details link for the update to be tested. This will display file information and let the administrator save the file to disk where it can then be installed manually on a test machine. The test machine should be a workstation comparable to computers that are being utilized in the network -- running the same software, but not be used for production work. It is also a good idea to have a server to test the updates on, especially if you plan on using Software Update Services to update the patches on any production servers. The test server should be one that does not perform any critical duties.

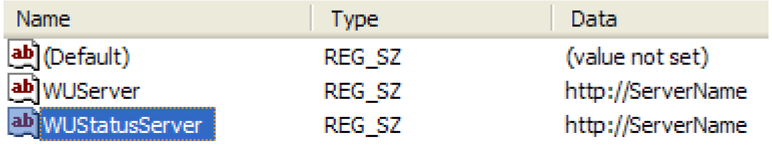
This level of testing is necessary because it is possible that the updates themselves can cause the client computer to have errors within the operating system or completely crash the operating system. For example, Microsoft released a patch on April 16, 2003 to prevent a buffer overrun in Windows kernel message handling (Microsoft Security Bulletin MS03-013). This patch slowed machines with Windows XP SP1 installed. If a patch like this was properly tested before deployment, the users would not be inconvenienced by the installation of the patch. (Microsoft then revised the update on May 28 2003, to fix this issue.)

If Software Update Services determines a patch does not apply to the particular computer then these updates will not be released to that machine. For example if a patch is released for Windows Media Service but the client does not have Windows media services installed the patch will not be downloaded to the client.

After the testing, the administrator has the option of approving or not approving the update. The updates that are approved are then made available to the Automatic Update Clients that are configured to check the SUS server. The updates that are not approved are simply not made available to the clients. Logs of the synchronization and approval are stored as XML files and can be viewed through the SUS administration web page. These log files show dates and times of the last synchronization and which updates were approved and which were not.

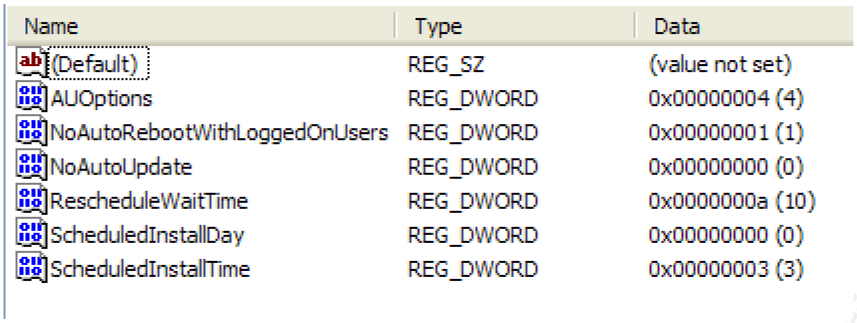
Client Configuration

Now that Software Update Service is installed and running on the server and Automatic Updates Clients are installed on the workstations, the administrator must now configure the clients. One way is to manually edit the registry on each client. To manually edit the registry open the registry editor and browse to "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" and add the following registry keys:



Name	Type	Data
(Default)	REG_SZ	(value not set)
WUServer	REG_SZ	http://ServerName
WUStatusServer	REG_SZ	http://ServerName

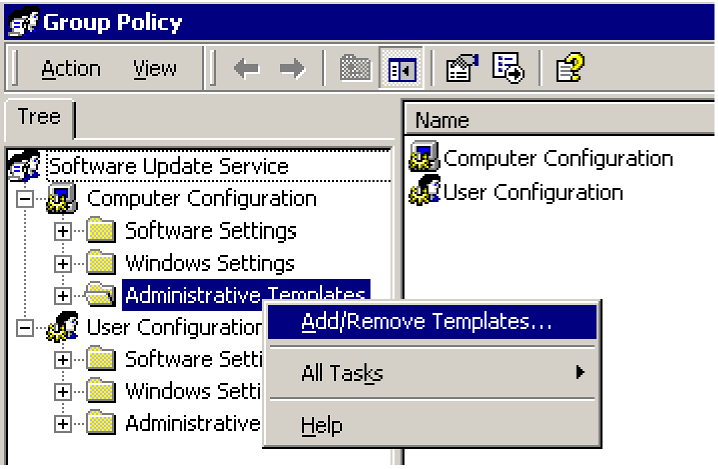
Then browse to “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU” and add the following registry keys:



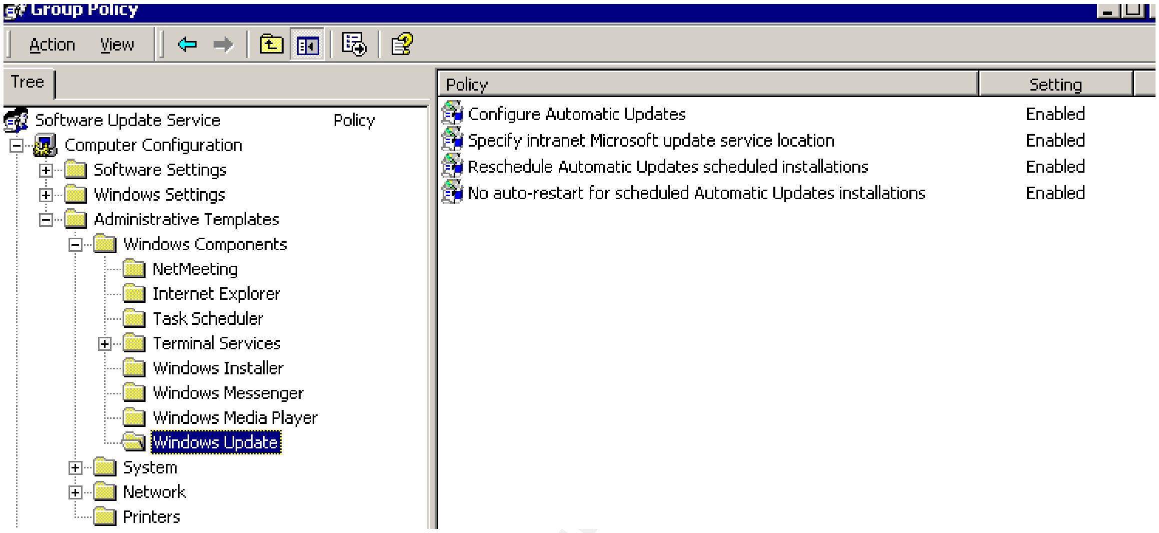
Name	Type	Data
(Default)	REG_SZ	(value not set)
AUOptions	REG_DWORD	0x00000004 (4)
NoAutoRebootWithLoggedOnUsers	REG_DWORD	0x00000001 (1)
NoAutoUpdate	REG_DWORD	0x00000000 (0)
RescheduleWaitTime	REG_DWORD	0x0000000a (10)
ScheduledInstallDay	REG_DWORD	0x00000000 (0)
ScheduledInstallTime	REG_DWORD	0x00000003 (3)

The values for this set of keys will vary depending on how the client is to behave and are included in the Software Update Services Deployment White Paper. An excerpt from the white paper detailing these settings is included in Appendix A.

As shown above, there are several registry keys that would have to be added to each machine to successfully setup the clients. A more efficient way to do this would be through an Active Directory Group Policy Object. To add this group policy, add the Windows Update Administrative Template to the Group Policy editor. This is done by first opening the group policy editor, and then right clicking on Administrative Templates under Computer Configuration. Click Add/Remove Templates to add the Windows Update Administrative Template. The template file is named “wuau.adm” and is located in the %systemroot%\inf folder.



The template adds the Windows Update folder under the Windows Components section in Administrative Templates. This will allow an administrator the ability to change the settings that the Automatic Update clients receive. There are four policies that can be used to change the behavior of the clients. If there are only two policies visible in this section then the most current version of wuau.adm should be downloaded at http://microsoft.com/downloads/details.aspx?FamilyId=D26A0AEA-D274-42E6-8025-8C667B4C94E9&displaylang=en. The current version of wuau.adm, as of this writing, is 5.4.3630.2550 and the file size is 25 KB. If you have an older version or one that is not 25 KB, there could only be two policies shown, limiting the settings that can be changed on the clients.



Policy	Setting
Configure Automatic Updates	Enabled
Specify intranet Microsoft update service location	Enabled
Reschedule Automatic Updates scheduled installations	Enabled
No auto-restart for scheduled Automatic Updates installations	Enabled

The first policy listed, "Configure Automatic Updates," gives the option to notify the user for downloads and installs. The administrator can set the client to download and install automatically or to prompt the user for the download or for the install. If the administrator chooses to not prompt for the download or install, then the time at which the client will connect to the Software Update Server and look for updates can be configured. The default setting is 3:00 am.

The second policy listed, "Specify intranet Microsoft update service location," sets the location of the software update server. It is listed as http://ServerName. The location of the statistics server will need to be set. (This can be the same location.) The statistics are stored in the Internet Information Service (IIS) logs on the server specified and should look similar to:

```
2003-05-28 11:48:23 --Client IP-- - --SUS Server IP-- 80 HEAD /iuident.cab 0305281148 200
        Industry+Update+Control
2003-05-28 11:48:23 --Client IP-- - --SUS Server IP-- 80 GET /iuident.cab 0305281148 200
        Industry+Update+Control
2003-05-28 11:48:23 --Client IP-- - --SUS Server IP-- 80 HEAD
        /selfupdate/AU/x86/XP/en/wuaucomp.cab 0305281148 200 Industry+Update+Control
2003-05-28 11:48:23 --Client IP-- - --SUS Server IP-- 80 GET
        /selfupdate/AU/x86/XP/en/wuaucomp.cab 0305281148 200 Industry+Update+Control
```

```
2003-05-28 11:48:23 --Client IP-- - --SUS Server IP-- 80 HEAD /iuident.cab 0305281148 200
          Industry+Update+Control
```

The third policy listed, “Reschedule Automatic Updates scheduled installations,” sets the amount of time the client will wait before it will install the newly downloaded updates. This needs to be set to allow the machine to fully boot before updates are installed. If the machine is not on when the updates are scheduled to be downloaded the machine will download the updates when it is booted next, but will wait the specified amount of time before these are installed. (When I set this policy on my network, I set the wait time to 15 minutes to allow the machine to go through the full boot process and let the machine have some idle time before it starts the install.) The intent is to decrease the amount of time the user will be waiting on the computer to boot.

Finally, the fourth policy listed, “No auto-restart for scheduled Automatic Updates installations,” sets whether the client will automatically restart after the updates are finished installing, if needed. In my install and testing, I enabled this setting. Enabling this policy will not let the client computer automatically restart, but will prompt the user to restart. The client will not check for updates until the next restart.

Securing the Server

During the installation of SUS, the IIS Lockdown tool and URLScan are both installed on the server to help further secure Internet Information Services.[iii] If either of these are already installed, the installation will not make any changes to their configuration. The SUS server has to be protected from every possible angle with several layers of protection (defense in depth), because the implications of a compromised SUS server would be disastrous. If someone were able to “hack” into the SUS server they could possibly inject malicious code into hundreds of client machines running on that network. That could be very destructive not only on the local network but these machines could be used to distribute this malicious software or code, such as an IRC bot or worm. A table listing the changes the lockdown tool makes to the active website, as listed in the Deployment White paper, is included as Appendix B. The installation of the IIS Lockdown tool is still not enough to consider your SUS server “safe”. We also need to check the patches on this server on a regular and frequent basis. As I have noted in the above paragraph, if this server is compromised, it only opens the door for many more machines to be compromised.

Now that Software Update Services is installed and configured, the server needs to be patched and locked down. The administrator needs to determine if this product does what is needed and is secure and reliable. SUS downloads patches from Microsoft, allows the administrator to test and approve these updates and then make them available to the workstations. I have one concern about the client configuration. The clients can only be set to check the SUS server once in a 24 hour period. If a critical patch is released early one morning, the administrator might test it at as soon as it is released, determine that it needs to be immediately deployed. However there is no way to force the clients to check the server or to push the update out from the server. If the clients are set to check for updates on the server in the early morning hours it could be almost a full day before the updates reach the client machines.

SUS will only install Windows Critical Updates, Windows Critical Security Updates, and Windows Security Roll-ups. According to Microsoft, a Critical Update is a fix to a critical problem that is non security related. Following this definition a Critical Security Update would be a fix to a critical security problem. A Security Roll-up is a combination of hotfixes, security updates, and critical updates. To install service packs or updates for other software such as Microsoft Office they have to be downloaded and installed manually.

Another issue with SUS that needs to be discussed is the ability to tamper with the files that are deployed to the clients. In a Case Study written by James McVicar[iv], he discovered that if an executable were renamed to match a Microsoft Update stored on the SUS server, the executable could then replace the update and it would then be pushed to the clients after it was approved. This could lead to any sort of malicious software being pushed out to the clients. The only way to prevent this from happening would be to make sure that no "bad guy" could gain access to the SUS server. There is obviously no guarantee that someone won't comprise this system at any time no matter how many precautions are used. McVicar's solution to this problem is to use SUS to approve updates but point your clients to Microsoft to download the updates. This solution may not be feasible if the workstations are not connected to the Internet. Administrators who are trying to preserve bandwidth because of slow connections or high traffic may also choose to configure their clients to download the updates directly from the SUS server.

If the clients are configured to connect to the SUS server for the updates, then other steps must be taken to secure and monitor the SUS server. There are several layers of protection available to secure this machine. The first thing that needs to be examined is the services running on the SUS server. The services that are critical to the operation of this server need to be determined, and any that are not necessary should be stopped and configured to not start up automatically. For example, if this is not an FTP server the "FTP Publishing Service" does not need to be started. After determining what services need to continue to run, then look at the connections that must be left available to the machine. This allows the implementation of a firewall between the SUS server and the Internet connection. If the only function of this server is to run Software Update Services then we can tailor our firewall to this. Software Update Services only uses outbound HTTP requests, so a “deny all” rule can be used and then only allow outgoing HTTP requests from that computer. If the SUS server will be performing other duties, then the firewall may need to have other “allow” rules added to accommodate those services.

Next to be discussed is host-based intrusion detection and prevention. For host-based intrusion prevention, the administrator can setup a personal firewall such as BlackIce Defender to monitor connections to the computer. BlackIce monitors connections to and from the machine and watches for abnormal or unusual activity and will alert the administrator to this activity. Antivirus software should also be installed and running on the computer to watch for malicious files. For intrusion detection on the host, implementation of file integrity checking software is necessary. A popular product to do this is Tripwire for Servers. Tripwire monitors the file system by comparing the current file against a baseline created by the user. This will alert the administrator to any changes made to critical files and/or data. These changes can then be analyzed to determine the source of the change.

The log files also need to be audited for unusual activity. On the SUS server the administrator should carefully watch the application, security, and system logs as well as the IIS logs. According to the GSEC courseware on day five, Auditing should be enabled on a minimum of the following events: “Logon and Logoff – success and failure, File and Object Access – failure, Use of User Rights – failure, Security Policy Changes – success and failure, and Startup, Shutdown, and System – success and failure.”[v] The security logs should be analyzed for excessive logon attempts. The application and system logs should be analyzed for entries from services that should not be running or from non-system processes.

Conclusion

Software Update Service can be a good product to help secure a network. SUS is easy to install on the server and on the clients. Configuration of the Server is very simple. The client setup is not difficult, but requires the administrator to research and decide which setup best fits the requirements on their network. Software Update Services helps automate a very important aspect of security – applying patches to the Windows operating system.

It takes more than patching software to be secure. The automation that SUS provides allows more time to focus on other layers of security such as firewalls, securing unnecessary services, host-based intrusion detection, network based intrusion detection, and host-based intrusion prevention -- to name a few. These areas are often neglected due to time constraints, and products like Software Update Service may allow administrators to spend more time focusing on them, and less time worrying about applying all those patches.

References and Resources

i. Microsoft Corporation. “Software Update Services” URL: http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

ii. The SANS Institute. “Mistakes People Make that Lead to Security Breaches”. October 23, 2001. URL: http://www.sans.org/resources/mistakes.php

iii. Fawcette Technical Publications. Scott Schnoll. “Stay Current With Software Update Services” October 9, 2002 URL: http://www.fawcette.com/reports/mec/2002/10_09_02/schnoll/default_pf.asp

iv. The SANS Institute. James McVicar “Use Caution When Deploying Microsoft’s Software Update Services On a Small Network” November 10, 2002 URL: http://www.giac.org/practical/GSEC/James_McVicar_GSEC.pdf

v. The SANS Institue. SANS Security Essentials V. Windows Security

Microsoft Corporation. “Software Update Services White Paper” January 29, 2003 URL: http://www.microsoft.com/windows2000/docs/SUSOverview.doc

Microsoft Corporation. “Deploying Microsoft Software Update Services” January 29, 2003 URL: http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

CNET Networks. James Michael Stewart “Microsoft makes software updates simple” URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2880514,00.html

InfoWorld. P.J. Connolly. “Patching made painless” URL: http://www.infoworld.com/article/03/03/21/12sus_1.html

Geek.com Brian Osborne “MS patch slows down Windows XP” URL: http://www.geek.com/news/geeknews/2003Apr/gee20030425019740.htm

Appendix A

An excerpt from “Deploying Microsoft Software Update Services” available at http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

RescheduleWaitTime

Range: n; where n = time in minutes (1-60)
Registry value type: REG_DWORD

NoAutoRebootWithLoggedOnUsers
Set this to 1 if you want the logged on users to choose whether or not to reboot their system
Registry value type: REG_DWORD

NoAutoUpdate
Range = 0|1. 0 = Automatic Updates is enabled (default), 1 = Automatic Updates is disabled.
Registry Value Type: Reg_DWORD

AUOptions
Range = 2|3|4. 2 = notify of download and installation, 3 = automatically download and notify of installation, and 4 = automatic download and scheduled installation. All options notify the local administrator.
Registry Value Type: Reg_DWORD

ScheduledInstallDay
Range = 0|1|2|3|4|5|6|7. 0 = Every day; 1 through 7 = the days of the week from Sunday (1) to Saturday (7).
Registry Value Type: Reg_DWORD

ScheduledInstallTime
Range = n; where n = the time of day in 24-hour format (0-23).
Registry Value Type: Reg_DWORD

UseWUServer
Set this to 1 to enable Automatic Updates to use the server running Software Update Services as specified in WUServer below.
Registry Value Type: Reg_DWORD

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate

WUServer

Sets the SUS server by HTTP name (for example, http://IntranetSUS).

Registry Value Type: Reg_SZ

WUStatusServer

Sets the SUS statistics server by HTTP name (for example, http://IntranetSUS).

Registry Value Type: Reg_SZ

Appendix B

An excerpt from “Deploying Microsoft Software Update Services” available at http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

Option	Software Update Server setting
Remove Script Mappings: ASP	Enable .ASP files
Remove Script Mappings: IDQ	Disable
Remove Script Mappings: SHTML, SHTM, STM	Disable
Remove Script Mappings: IDC	Disable
Remove Script Mappings: printer	Disable
Remove Script Mappings: HTR	Disable
Remove Sample Web files	Remove them
Remove Scripts Virtual Directory	Remove them
Remove MSDAC virtual directory	Remove it
Disable WebDAV	Disable WebDav
Prevent IIS anonymous user from executing system utilities	Prevent it
Prevent IIS anonymous user account from writing Web content	Prevent it
Parent path	Disable it