Global Information Assurance Certification Paper

PLANNING AND IMPLEMENTING A PATCH MANAGEMENT SYSTEM USING SUS AND WINDOWS UPDATE.

Steve Picard
November 15 2003

PLANNING AND IMPLEMENTING A PATCH MANAGEMENT SYSTEM USING SUS AND WINDOWS UPDATE.

ABSTRACT

The purpose of this paper is to satisfy the 1.4B practical requirement for the SANS GSEC certification. I will give some of the main reasons why a business would want to be proactive in patch management. Also some of the many different ways to set up a SUS and Windows Update patch management solution. It is beyond the scope of this paper to include every possible implementation, and feature of SUS and Windows Update. It is the intent of this paper to give someone the knowledge to create and customize their own patch management systems.

INTRODUCTION

The time for exploits of known vulnerabilities to be released is continuing to decrease. In some cases it is only a few hours from when vulnerability is released to when there is an exploit to use that vulnerability. Even though it is a little dated, there was an article from CNN that noted that most exploits are exploiting known vulnerabilities. Even in 1999 it was realized if you could close those known holes you would be much less susceptible to being infected with viruses and Trojans. It is worth a short read

http://www.cnn.com/1999/TECH/computing/12/17/hack.exploit.idg/

WHY PATCH?

Since most corporations toady are always looking to cut cost and have greater return on investment for their shareholders. It is a sad fact that the IS department is one of the first departments to be forced to be more effective. With these pressures, very few IS departments today have the resources to go machine to machine and patch their machines by hand. This opens up the company for a dramatic loss if an exploit were to be malicious.

As we all know it is only a matter of time before our work environment is contaminated. Your environment may become contaminated through every thing from a sales person bringing back an infected laptop into the organization or a person that works from home using the corporate VPN and then goes off line and becomes infected and reconnects again with an infected computer.

When you are infected how will you act? What will you have in place to limit your loss? There are an increasing number of precedent setting cases especially in the US where companies are suing other companies for being negligent and causing down stream liability. It is something only the courts will decide what it means to be negligent causing harm to intellectual property and resources, but

as security professionals and administrators we should make sure we are a good citizen to other companies and don't cause harm to other businesses.

Windows update and SUS should be used to give a reasonable expectation that your corporate machines are patched before an exploit is released. As the functionality of SUS continues to increase this is becoming an important piece of a defense in depth model. By patching your desktop and servers with the newest patches you will be reducing your exposure to potential risk from everything from lost data to down time for your IS group and users having to clean the infected machines. So what are the best practices involved in deploying SUS? First let's look at what is needed.

CREATING THE SOLUTION

It's the combination of the Windows update client and the SUS server that work together to allow you to proactively install patches. Your SUS Server(s) is where you will choose what patches you will publish for client installation. There will be times you may choose not to install patches for such reasons as if a patch interferes with an application. The other half of your patch management system will be the configuration of the Windows update client. There will be several different options one can use to configure the way the clients behave. You can configure everything from when your machines will query the SUS server to the automatic install and reboot of client machines.

Unfortunately this method of patch management is only focused on windows 2000, XP and newer machines. So if your environment includes several NT machines I would highly suggest the removal of these ASAP. Or at least know you will need some other form of patch management for those NT machines. It is important to realize that one un-patched machine can be a source of infection. One attack does not necceicarly use the same exploit that machine was infected with to infect other machines when they are on your network. I realize in some environments the removal of the remaining NT machines may be difficult, but this should be planned as soon as possible. If the removal of NT machines from your environment is not feasible I would highly suggest you seriously consider implement a SMS server to take care of these machines.

Now that we have the basic plan down as how this is to work the next logical progression is to ask how we are going to use our SUS servers and the Windows Update to patch your windows 2000 and XP machines. The Windows Update client is included in SP3 for windows 2000 and windows XP SP 1. From the client side all that is needed is the editing of a few registry keys to point to your new server. We will deal with the client configuration first since it is the easiest. Since group policy will in effect modify registry keys I will only deal with what the registry changes are and what they do. The following link gives good information on how to use local group policy and active directory to attain the same result. I recommend its reading.

http://support.microsoft.com/default.aspx?scid=kb;en-us;328010

WINDOWS UPDATE

All Windows update related registry keys can be found at the location below and its sub keys.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

There are 2 keys under the above root. These 2 keys allow you edit what SUS server you want to use. Both for notifying your client of new updates as well as where it will download them from. Generally the value of these will be the SUS server. However if you decide to have an alternate content distribution point you will need to change the **WUServer** to reflect the distribution point. But will still need to leave the **WUStatusServer** to the windows update server. This is where your client will poll the Windows update server to see if there is new updates to download then pull from the server in the in the **WUServer**.

Under the **AU** directory there are more keys you will want to edit. Below is a brief description of the keys as well as what they do.

NoAutoUpdate: This can be one of two options. If this value is set to 0 updates are enabled. If set to one they are disabled obviously we want them enabled so we will want to set this to 0

AUOptions There are 3 possible options here, the acceptable values are 2, 3 and 4. If this value is set to 2 this allows us to notify the user there are new updates to download and be installed. If this option is set to 3 you can have the client machine automatically download the updates then notify the end user that they need to be installed. The third option is setting this value to 4 this option automatically downloads and installs the patches and installs them silently finishing the install when the user reboots their machine.

ScheduledInstallDay This value can be set to any thing between 0 and 7. If set to 0 the windows update service will check every day for new updates. If set to a value between 1 and 7 it will only check on that particular day of the week. Where 1 is Sunday and 7 is Saturday.

SchedualedInstallTime this option can be set to anything between 0 and 23 this is meant to allow machines to query the server at a specified time of day where 0-23 is the hour of the day in a 24h clock. This could be especially useful with desktop machines that are left powered on during the evening hours.

UseWUServer this option can be set to 0 or 1 if set to 0 the machine will go to the Microsoft windows update site to download the updates. As we want our clients to point to the SUS server we create we will set this to 1.

ReschedualeWaitTime is the time windows update will wait to install the patches from when they are downloaded. This just allows you to customize when the patches will be installed. It is suggested that this be used in a highly managed environment.

NoAutoRebootWithLogedOnUsers the default for this option is set to 1 this means windows update will not reboot the machine with a user logged in. Set to 0 windows update will automatically reboot the machine even with someone logged in. This option in my opinion should only be used in an environment where people are told they need to save all work at the end of the day and log off. With this registry key set to 0, the machines will be rebooted with the users only having 60 seconds to save their work.

Now that we know what the options do the following are suggestions on how to configure your clients to have an effective patching process. Once you have your machines pointing to the SUS server and the clients are updating. I would suggest changing the AUOptions value to 4 ensuring automatic download and instillation of the patches. I would then leave the SchedualedInstallDay at 0 so the SUS server is queried daily. If you decide to set the scheduled install time I would highly recommend for laptop users a time during working hours. I would even go as far as limiting the time between 2 hours after the start of work and 2 hours before the end of the workday this allows users to come in late and leave early and still query the SUS server. Of course if you are going to go through the trouble of setting up a corporate SUS server(s) you will need to change UseWUServer to a value of 1. Generally I don't see a need to change the ReschedualWaitTime in the corporate environment so I recommend no change. To limit hatred towards the IS group and rioting users I would leave the NoAutoRebootWithLoggedOnUsers option to 1 where it will not reboot the machine if someone is logged in. The only possible way I would consider using this option is if your clients were set to query the server during the evening hours and all users were told they must save their work because their machines will be rebooted nightly. As you can see there are many options on how we can configure our clients. Generally it should be advised that with any patching process less user intervention does create a more secure environment. As well when creating a deployment model generally simpler is better. Now that we have the information on how the above values can be set to customize our clients we now need to look at how we will install our server(s).

THE SUS SERVER

The SUS server is the next component in a Windows Update and SUS environment. This is where your desktop machines will go to get their updates. The minimum requirement for your server is. A PIII 700 with 512 MB of RAM and a minimum of 6 Gigs of Hard drive space for the security patches. (This will continue to increase so proper planning should be done for the lifecycle of the

server.) Microsoft says you should be able to service 15,000 clients using this configuration. Although the environments I work in have fewer machines per site, than Microsoft's recommendation, I would recommend keeping the number of machines your SUS server services down to 1000. Especially if you are planning on using a machine that just meets the minimum specifications. You will need to have Windows 2000 or newer server installed on this server as well as IIS 5 or newer. If you do not already have the IIS lockdown tool installed It will install it for you with the install of your SUS server. If you already have the lock down tool installed the SUS installation will skip this step not making changes to your instillation of the lockdown tool.

PLANNING YOUR DESIGN

Once you have the above or better set aside for your new SUS server(s) you can start the install of the server end of your windows update solution. But before we get to he install you will want to map out the logistics of your server model first. In an Organization under 1000 employees in one office you can probably implement a single site model. For those in larger organizations and geographically distributed offices I would highly recommend a distributed model.

You can install as many SUS servers as needed to fit your organization. It is generally advisable to use one point of publishing or approving patches and have the other internal SUS servers look to that one server to get their information.

When you are planning the server end of your deployment there are many things you will need to take into consideration. You will need to look at such things as the size of the company. As well as population and geographic distribution.

In order for a patch management system to work effectively you will want to plan your model to work for your enviroment. In a large organization it would be agreeable to have several dedicated SUS servers. You will want to make sure every site in your company has an install of the SUS server. In the smaller locations of 20 or 30 people you may be able to install this on an existing File server depending on the current usage of the server. In extremely large organizations a combination of models may be beneficial. What ever your situation a little proactive planning now, will greatly improve the usefulness of your implementation in the future.

Once you have done your proactive planning the actual Install of a server is relatively easy. After the OS and IIS installed you just need to go to the SUS site from Microsoft. And download the install package…..

SECUREING AND CONFIGURING YOUR SERVER

By default the administration console is run from a website on the new server. This URL will be http://<servername>/SUSAdmin. This site can only be used by individuals that have administrative privileges on the local server. It is my opinion that this administration page should be replaced with a secure web administration site. You will want to use the HTTPS/SSL protical to prevent information including credentials from being sent in clear text if you chose to administer your server from your desktop or from a computer outside your organization.

In order to implement this you will need a SSL certificate. Once you have received or created a SSL certificate you should then move this certificate to the local server you will be running SUS from. In order to apply the certificate into the administration website you will need to go to the properties page of the website under the IIS admin snap-in. Select the properties page of the website and set SSL to port 443. Then on the directory security tab, select server certificate. This should start the web server certificate wizard. On the first screen click next, and then select the option to use an existing certificate. Choose next, and then select the certificate you created earlier. And select next. Then select next and ok to close the last box.

Now that you have the SSL certificate installed on your server you will now need to select the directories you want SSL to be enabled on. You will want to enable security on the following folders. The following will generally be under the main website on that server unless you specified otherwise.

\autoupdate\administration
\autoupdate\dictionaries
\shared
\content\EULA (This folder will only appear after the first successful sync)
\content\RTF (This folder will only appear after the first successful sync)

To use the certificate you will need to go to the snap-in for your IIS server and select the properties of the above sites and on the security tab select use SSL.
If this has been implemented correctly you can now go to your new secure admin page at:
HTTPS://<servername>/susadmin

TESTING THE PATCHES

Since you now have your clients and your SUS server installed you now can push all the patches you want to your client machines. But before you do that, there is a principle you will want to take into affect that's CIA Confidentiality Integrity and Availability. We have already dealt with Confidentiality with the implementation of the SSL in the administration of our admin pages on the SUS Server, but before we push out content to our users machines we would want to make sure the patches work on a few machines before pushing it enterprise

wide. This will help guarantee that if there is a problem it gets addressed with out taking down your entire organization, or an entire department. Thus guaranteeing the availability and integrity of the client machines. It is most advisable to take a few machines in each department and have them update directly from the Microsoft site or manually go and install the patches on their machines to see if there are any problems with the patch. Generally if after a day or so there is no problem reported it is safe to push these patches enterprise wide. Having a well thought out model will help here. If you have one point of approval with in your organization this will cut down on the administrative duties needed to install the patches in your environment. In most implementations a hierarchical implementation will be beneficial. So once you have gone through done some proactive testing on the patches you just need to go to your administration website and select to publish the patches to your clients. And generally with in 24 hours 95% or ideally more of your machines will have queried the SUS server and at least notified the users that there are patches ready to install.

EXPANDING AND SCALLING

As your corporation grows, and you start to see more and more strain on your servers. You will want to install more servers in your environment. Since we have already discussed how to install a SUS Server I will not go over that again. But there are some changes you will want to make to the new child servers you install. One of those changes is setting up your new servers to get the patches from your local site publishing server. As well there may be a need to have your SUS servers utilize load balancing and create a SUS cluster.

For this to happen you will need to have the “parent” server, or the one that receives updates from the Microsoft Windows Update server need to be set to save updates to a local folder on the set options page. As well this server will need a copy of all the updates for all your locals. If they are not there your “child” server will not be able to download these patches from the parent, and the sync will fail. On your new child server you will need to select **Synchronize list of approved items updated from this location.** Once this is selected the child server will pull a copy of the content from the parent server. Setting your child server to update itself with the approved updates from a parent server in your organization will take away the functionality on that new child server to approve updates. So if you are going to use a child parent topology you will need to know you will not be able to approve patches at a parent level then unapprove them at a child level.

In exceptionally large environments you may have a need to have several child servers in a single location. It may also be a good practice in your environment to load balance these servers. This will bring several benefits including allowing the servers to share the load of the request from your clients and reduce network traffic and stress on the local LAN. We can do this relatively easily using the load

balancing functionality included in windows 2000 server and newer. The following is an advisable read if you plan to implement this in your environment.

But the basics are you will need to setup your child servers to maintain a copy of the content they will disperse from the parent server. As well as enabling the load balancing service on all of the child servers in that site. And hopefully all is well. I do not have the opportunity in this paper to go into great depth as how this can be configured but I would defiantly suggest the reading of the following from Microsoft on the installation of the load balancing service as well as the portion of the SUS deployment guide also available from Microsoft.

Well hopefully all went well when you mapped out your SUS organization and dealt with the need to create an enterprise based patch management system. As a wrap up I would highly suggest spending lots of time on the Microsoft website looking at the above articles. As well as the Microsoft security website at Http://www.microsoft.com/security/ this website has lots of useful information on how to make your SUS implementation work better for your organization.

Once you have a SUS implementation in place it would be a good idea to have some way of ensuring the patches are getting installed on your machines, and correct any problems you may be having. There are many 3rd party tools on the market like Shavlik's HFNetChkPro and even Microsoft's Baseline Security Analyzer can be used for these purposes.

CONCLUSION

The need for patch management will only become a greater and greater need and responsibility for organizations in the future. There is increasing opportunity for loss from companies not only from the cost of down time but of the potential of being charged with down stream liability for the loss of other companies due to your negligence. As the first attempts at these law suits are getting to be lengthy battles they are also setting precedent around the world for future law suits from people and companies affected by an individual person or company's negligence to patch their systems and prevent acting as a propagation point for viruses as well as being used as zombies in DDOS attacks. Since the legal meaning for negligence includes a failure to exercise the degree of care considered reasonable under the circumstances, resulting in the unintended injury to another party. Even with out knowing it your company to could be opening itself up for a potential negligence suite. The following link has some very interesting reading regarding denial of service attacks and their impact.

What the future holds is unclear for potential down stream liability and what will be considered reasonable care for preventing things like viruses. I would think it is probably inevitable that there will be increasing lawsuits and there will be some sort of precedent set eventually that people and corporations can be sued for

damages to intellectual property and lost revenue from downed sites ETC. But even If it is eventually proved that the companies being sued for down stream liability were doing all that was reasonable to contain the viruses on their systems you as a responsible admin or security professional will want to make sure you have some form of patch management. If nothing else to reduce loss to your own company. The one drawback I see with the currently available version of SUS is that clients are only set to update every 22 hours plus or minus a random number. If there were an exploit to come out within hours of vulnerability being identified the current SUS system would not be able to deal with it. It is rumored that in the next version of SUS you will be able to choose to push patches to your clients, but we will need to wait for that.

In conclusion your organization will only benefit from using SUS to patch your systems. And as Microsoft puts more functionality into SUS the value of SUS will only increase.

REFFRENCES

Gaudon, Sharon "**Virus Damage Worst on Record for August"**
ITMANAGEMENT September 2, 2003
http://itmanagement.earthweb.com/secu/article.php/3071051

Microsoft Software Update Services Home Page
http://go.microsoft.com/fwlink/?LinkId=6930

Windows Clustering Technologies—An Overview
Microsoft November 2001
http://www.microsoft.com/windows2000/techinfo/planning/clustering.asp

Johnston, Margret **Known vulnerabilities are No. 1 hack exploit**
CNN December 17 1999
http://www.cnn.com/1999/TECH/computing/12/17/hack.exploit.idg/

How to Configure Automatic Updates by Using Group Policy or Registry Settings
Microsoft June 4th 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;328010

Downstream Liability forAttack Relay and Amplification
Adaptation of a presentation given at a RSA conference in 2002
http://www.isalliance.org/resources/papers/Downstream_Liability.pdf

Microsoft SUS deployment guide
Microsoft January 2003
http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

Flynn, Wayne **SUS Servers is your SUS Server working?**
SUSSERVER January 27 2003.
http://www.susserver.com/FAQs/FAQ-IsYourSUSServerWorking.asp

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event