GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Case Study:

Patch Management Philosophy and Implementing a MS Windows Patch Management and Remote Quarantine System Using Readily Available Technologies

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

SANS Security Essentials GSEC Practical Assignment

Version 1.4c – Option #2

Adam G. Robinson

October 26, 2004

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract 1

Background 2

Security and Patch Mgt at ABC Corporation 3

The Good Turned Bad 2-3

What can be done in the future? 4

How it works 5

Requirements 5-6

Setup 6-9

- MS Windows Software Update Services Servers 6
- MS Windows Server 2003 6
- Connection Manager Administration Kit (CMAK) 6
- Script 8
- SQL Server Setup 8

Setup Summary 9-10

Result 10

References 11

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Abstract

Patch management has been a topic of great debate over the past few years. The questions of patching or not patching; Do you risk bringing down a system or application because of problems with patch, or do you risk your whole infrastructure or data because a virus entered your environment because you did not apply a patch.

This paper is a case study at a place that I have worked, ABC Corporation. Their philosophy in the beginning was the older, more common approach of not applying patches to desktops, and this paper will show how that policy effected the organization as a whole. Also, I will outline the steps we took and the technologies we used after the fact, to ensure the organization was not effected again while faced with major budget restraints in a slow economy.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Background

ABC Corporation is a company that produces products and provides many services to its customers. It has many employees that work out of their home, work in other companies, and travel frequently. The services in which it provides are global, with remote offices throughout the United States and in many different countries throughout the world. The employees at ABC rely heavily on technology, communication, and services at the corporation's headquarters. As a result, these employees on the road and in the different locations require a means to remotely connect to these services and data 24 hours a day 7 days a week. The global and remote offices connect back to Headquarters one way or another, whether it is a T1 line or Internet VPN. The traveling employees connect to the office through dial-up or VPN connections.

Security at ABC and its Patch Management Philosophy

ABC Corporation had identified the need for security in their organization and regularly conducted security meetings to discuss IT related security. The security at the organization was solid for the type of organization that it was. It was lead by a Chairman and about 5-8 team members who were part of the administration team. The organization underwent a wave of job turnover but they had great track-record of zero downtime due to security related incidents year after year.

The patch management philosophy of the security team at the time was not to patch the desktops and some servers because of problems that patches may cause with vendor specific software. As IT professionals at ABC we have all witnessed systems and applications having problems after applying patches and the security team decided it would be best to patch only the systems that could come under regular attacks (the firewalls, etc).

The Good Turned Bad

While this patch management philosophy worked for years. A simple virus that ceased operation at the company for a few hours would change the way ABC would look at this problem forever.

I had just received good news about one month previous to the virus that I was going to take over the job as Chairman of the Security Team. My boss Brian, who was manager of Information Systems at the time, had the job for a couple of months after the previous Security Chair left the company. While Brian enjoyed the position, he had a heavy workload and could no longer handle the time required to run the security team, so he passed the job on to me. While a great

© SANS Institute 2005 Author retains full rights.

opportunity at the time, it ended up turning into a very rocky start at a job I had so much energy and ideas for.

About 3 weeks into the position the network went down because of a strand of the Welchia worm. *Symantec's Security response center* summarizes the virus as and what it tries to do as follows:

- Attempts to download the DCOM RPC patch from Microsoft's Windows Update Web site, install it, and then restart the computer
- Checks for active machines to infect by sending an ICMP echo request, or PING, which will result in increased ICMP traffic
- Attempts to remove W32.Blaster.Worm

This virus propagates by taking advantage of a security hole in MS Windows based computers as outlined in Microsoft Security Bulletin MS03-026 (Buffer Overrun in RPC Interface Could Allow Code Execution). This virus would take advantage of the vulnerability, scan for and try to clean up the W32.Blaster.Worm if infected, and then attempt to find other pc's to propagate to using ICMP echo requests. While a simple ICMP echo request would not cause too many problems, the rate of speed at which this virus moved through the network was alarming. These pc's used all of their processing power to locate other hosts and before long one pc turned into 1,000 and the network equipment could not keep up with the traffic. The Distributed Denial of Service attack stopped the network and all of the services on it.

The cleanup process included finding what the problem was, disconnecting the server farms from the closet switches, visiting each and every desk to clean the pc's and reattaching clean pc's back to the network. This was a very lengthy process and the whole team worked a 30+ hour shift. The only positive about it was the virus hit late in the day so most users were heading home.

While a very long night that I would never like to experience again, I learned quite a bit from this experience. The first thing is the good and bad side of technology. Remote technologies such as VPN allow people to connect from anywhere in the world at any time, but they also have their downside. The biggest problem that Information Systems Professionals have to deal with is not being in control of the pc's that leave the office. Remote users are connecting to so many networks, from the airport, to their home DSL or Cable modems, to allowing their son or daughter to use Instant Messaging or Peer to Peer software, and then the pc's are plugged back into the corporate network and next thing you know, the whole network is down. The next thing I learned and probably most important from the incident is how important it is to have a disaster recovery and Business Continuity Plans in place. While the team performed very well and brought the company back online very quickly, it was faced with making "what is best for the company decisions" at the same time we were trying to fix other problems. If the plans would have already been in place, we would have had a much easier time

© SANS Institute 2005 Author retains full rights.

and the Information Systems department would not have had to make business decisions at 3 am of what is best for the company. The company could have made these decisions earlier under ideal circumstances.

What can be done in the future?

Even though this was a great learning process, steps need to be taken to prevent problems like this from happening again. Since virus writers are targeting exploits faster and faster and they are targeting the ones that cause the most damage, un-patched pc's are more vulnerable then ever. This creates a very tricky scenario for IT Professionals. With today's traveling worker, who is spending more and more time on the road and connecting to the network sometimes only once or twice a month, how do you make sure that these machines are kept up to date before they connect to the office? How do we prevent the next W32.Welchia.Worm from invading the network? While not totally possible to make your network one hundred percent safe, Defense-In-Depth teaches us that we must take all reasonable precautions to prevent problems from happening.

As the new Chairman of the Security team, and under serious budget constraints, myself and the security team researched solutions to this problem. I remembered back to a new technology that I heard about while attending a Microsoft Conference in early 2003. They spoke about a new technology that would be included in their Windows Server 2003 implementation of their VPN. This technology would ensure remote users connecting to the network via VPN or RAS complied with a certain set of criteria and will place non compliant systems in a Quarantine area until they meet the corporate policies. Policies that can be enforced are checking to see if the computer has anti-virus installed, if it is running and has the latest definitions, if the pc has all the latest approved security patches for your environment, or just about anything you can script out. If the pc fails the check, it can be redirected to a webpage where it can fix the problems and then reconnect when fixed.

Another technology that was just becoming available was their internal Windows Software Update Server. This technology would allow a corporate IT Department to push out Windows patches to pc's with or without user intervention. When patches were released, they could be tested in a lab with corporate used applications and when approved, they could be pushed to all the pc's on the network. What about the traveling worker? With the quarantine server, we would prevent the users from connecting to the network until they install the patches or become compliant to the policies.

With this solution, the pc's in which we had limited control, now could be forced to be kept up to date. The road worker would be denied access if they did not comply with the policy. If the pc was found to be non-compliant it would be quarantined and sent to a webpage, where they could download the required

© SANS Institute 2005 Author retains full rights.

updates and then reconnect. All of the other pc's in the building would get Windows Updates and Anti-Virus as they always have and the network security would increase. While not totally free, this is a very cost effective solution. Microsoft's Quarantine Server technology is built in to Windows Server 2003 and Windows Update Sever is offered as a free download on Microsoft's website.

How it works

When a remote client initiates a VPN or RAS connection to corporate headquarters, the system verifies the user against the account database. When access is granted a popup dialog appears on the screen letting the user know their system is being scanned. In the background a script is being run using the Microsoft's MBSA client to check against Headquarter approved Microsoft Patches. Also, the script can check for things such as Anti-virus definition files and if Anti-virus is installed and running. If the system fails the check, a webpage pops up and lets the user know they don't have the correct updates to be allowed onto the network. At this time, the user cannot perform any actions on the network except for talking to the Quarantine Server. Further, a webpage is populated with the missing patches and/or missing anti-virus definition files and pops up on the users screen. The user clicks on and installs the missing patches and attempts to reconnect to the network. When the user connects again, the user goes through the same process again, and instead of being quarantined, the user is shown a success message and is able to proceed onto the network.

Requirements

The requirements listed below are the requirements for ABC Corporation's implementation of MS Quarantine services. The items marked with a * are optional. Since the quarantine checking process is script driven, other technologies may be used in its place.

Client Operating Systems

The remote access clients must be running Windows Server 2003, Windows XP or XP Home, Windows ME/2000/98SE.[1]

Server Requirements

Server in the Windows Server 2003 family which supports Routing and Remote Access

*Two Servers in which you can host internal Windows Update Services. One will be used for Windows Patches that can be pushed to clients, and the other will be used as the quarantine remediation server.

Software

© SANS Institute 2005 Author retains full rights.

*The latest version of Microsoft's MBSA client. The MBSA client will be used to quickly scan the pc for patch level and compare it against the internal Windows Update Quarantine Server.

*SQL Database. This database will be used populate the remediation quarantine webpage with proper patches so users do not have to visit Windows Update. When they are quarantined, this webpage will popup in a browser window on their machine telling them which patches they need with links to download and install.

Connection Manager Administration Kit (CMAK)- This will be used to construct the VPN client which will be used by the clients. It will run a post-connection action which will kick off the network policy requirements script and contains the notifier component which indicates a success.

A notifier component- The notifier component sends a message that the user has met all the requirements and can be passed through the quarantine. You can use your own notifier component but there is one provided with the Windows 2003 Resource Kit (Rqc.exe).[1]

Setup

MS Windows Software Update Services Servers

The first step in the setup process is to install and setup a MS Windows Software Update Services Server. You can download the latest version of the software at http://www.microsoft.com/downloads and by searching for Software Update Services. On the download page is a deployment guide white paper with instructions to setup the server. You will need to setup two servers following your corporate standards with Updates Services. One server will be used as the central server to push out updates to the organization. The other server will be set to synchronize with the main server and will be used as the quarantine server.

MS Windows Server 2003

Install and setup a MS Windows Server 2003 based server that will be used as the VPN Server. Remember to shut off all unnecessary services and to adhere to your company's standards and security templates for servers in your organization. Next follow the instructions below to setup Routing and Remote Access for MS Quarantine Services.

1. First you will need to create two user groups that have access to VPN so you can control who has access. Create one that will be called something similar to "Users with VPN Access" and another that is called "VPN Access Quarantine Bypass" (or something similar). The VPN Access

© SANS Institute 2005 Author retains full rights.

Quarantine Bypass will be for users that you do not want to go through the VPN Quarantine (I would recommend using this group for emergency situations and testing only). Now add the users that you want to have access to the VPN.

2. Routing and Remote Access is installed but not started or configured by default. Navigate to it and launch the program through the Administrative Tools menu in the start menu.
3. With the server name highlighted, select Action and then Configure and Enable Routing and Remote Access.
4. Walk through the wizard using the configurations options for your network and start the service.
5. In the MMC for Routing and Remote Access, right click on the Remote Access Policies line item. Select New Remote Access Policy.
6. Walk through the wizard selecting options that pertain to your environment and name the Policy "Quarantine Policy" (or something similar) and add the user group "Users with VPN Access" with permissions.
7. At this time you will create a second Remote Access Policy called "Quarantine Bypass" (or something similar). You will give access to this policy only to the "VPN Access Quarantine Bypass" user group.
8. Next, right click on the "Quarantine Policy" which you created in step 6 and select properties. Click the "Edit Profile…" button in the middle of the window. Select the advanced tab. Click Add..
9. Now you will need to add two profiles. The first one is called MS-Quarantine-Session-Timeout. Enter a value (in seconds) and click ok. This policy specifies how long a connection can remain in a restricted (or Quarantined) state before being disconnected.
10. The second profile you will need to add is called MS-Quarantine-IPFilter. This policy specifies what traffic is allowed on your network by a pc in a quarantined state. You will configure this to allow which ports you would like to communicate on your network and to what IP Addresses while a pc is in the quarantined state. This is to allow you to direct users to a website to remediate or fix their problems and to communicate with the quarantine server. Add any input or output filters you require to talk to the desired addresses.
11. Finish configuring your VPN objects with the other options that are required for your network.

© SANS Institute 2005, Author retains full rights.

Connection Manager Administration Kit (CMAK)

The CMAK is provided in Windows Server 2003. Add and configure it by following the steps below:

1. Navigate and launch the add/remove windows components from add/remove programs in the control panel.

© SANS Institute 2005 Author retains full rights.

2. Select the Management and Monitoring tools entry and click the Details button.
3. Check the Connection Manager Administration Kit and select Ok, click Next, then Finish.
4. Navigate to Administration Tools from the Start menu and select Connection Manager Administration Kit.
5. Follow the wizard and answer the questions. The selected options will be different based on policies and network setup at your organization.
6. Pay special attention to the custom actions page in the wizard. **This is where you will specify the post-connection action to run the script with the required parameters. Be sure to include the script and the notification component in the profile**. (*Special note- you may want to include a script that pulls the quarantine script from the quarantine server. This way, you can change what the script does without having to re-issue a new client every time).
7. Distribute this client to your Windows based machines.

Note: Remote access clients that do not install the new client are unable to obtain a normal remote access connection. They are placed in quarantine mode, and because they do not run the script or send the notification, are left in quarantine mode until the quarantine time expires, at which time they are automatically disconnected.[1]

Script

There are many things you can do with the script to quarantine pc's. A good place to start is Microsoft's website. They have some sample scripts for verifying client health configurations at:

http://www.microsoft.com/downloads/details.aspx?FamilyID=a290f2ee-0b55-491e-bc4c-8161671b2462&DisplayLang=en.

ABC Corporation implementation uses a script and the Microsoft's Baseline Security Analyzer client to verify against the corporate Software Update Services Server. This makes sure the pc's meet the approved corporate patch levels. The pc's which fail are quarantined and instructed to fix. The pc's which pass are allowed on the network.

MS SQL Server Setup

This step is optional. This is ABC's implementation of how it populates it remediation webpage for users when they are in quarantine. You may choose a different way.

This stage of the setup involves using SQL Server to import text files from Windows Software Update Server in order to lookup and populate a webpage to

© SANS Institute 2005 Author retains full rights.

remediate a quarantined pc. By default, the text files that are used to associate patch names with Operating Systems and program names are in the following directory on the Software Update Server:

\Inetpub\wwwroot\dictionaries\autoupdate

In this directory you will find folders for IE5, IE6, Win2K, WinXP, etc. These directories each contain text files which **associate patch numbers with update numbers**. Using a DTS Package in SQL and a few simple transformations you can extract the information you need from these text files to populate the tables desired. Now you are ready to create the remediation webpage. Use the SQL Tables with the associations to compare against the output from the MBSA client and match them up with the desired patch and create links to them from the webpage. Now when a user enters quarantine, the script fires this webpage on their pc and the patches that are missing are displayed and ready to be installed. As always, users can be instructed to visit Windows Update instead. This site is only for convenience to the user.

Setup Summary

Below are a summary of the steps of how everything works together:

Administration Summary:

1. The IT Administrator will create a packaged VPN client using CMAK
    a. The package will contain a script which will look for non-compliances.
    b. Also, the package will contain the notifier (Rqc.exe).
2. The VPN client will be distributed to all the users who will need to connect remotely
3. The IT Administrator will determine how to notify the user if their pc is found to be non-compliant and include it in the post script.
4. The IT Administrator will need to configure Routing and Remote Access to include the MS-Quarantine Policies.
5. The IT Administrator should setup a system to push out Windows Patches to its clients on a regular basis after fully testing them.

What remote users can expect:

1. A user will login to the network using the VPN client that is given to them that was created above.
2. Once authenticated a user enters quarantine mode.
3. While in quarantine, a post login script is run which checks for non-compliances and either grants the user access by issuing the notifier to the VPN Server, or redirects the user to a place that will give instructions of how to become compliant.

© SANS Institute 2005 Author retains full rights.

4. The user follows the directions and clears quarantine upon reconnection.

Result

After implementing this technology, users will no longer be able to connect remotely to the corporate network with a pc that is not kept up to date and possibly infect the network with a virus. Since the Wechia worm hit the ABC Company network, I have led the organization in creating a Business Continuity Plan and implemented this quarantine technology. While the company or any company is never one hundred percent secure, this technology is just one step in Defense in Depth. If another outage should occur because of the crafty virus writers, the ABC Corporation now has a Business Continuity Plan to follow.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

References

1. The Cable Guy, “Network Access Quarantine Control”, The Cable Guy - February 2003, Microsoft TechNet. http://www.microsoft.com/technet/community/columns/cableguy/cg0203.mspx

2. Frederic Perriot and Douglas Knowles, “W32.Welchia.Worm”, July 28 2004, Security Response Center. http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html

3. Microsoft Download Center http://www.microsoft.com/downloads/details.aspx?FamilyID=a290f2ee-0b55-491e-bc4c-8161671b2462&DisplayLang=en

4. Microsoft Windows Server 2003 Launch Seminar, Detroit MI, Cobo Hall, May 2, 2003.

5. Microsoft Windows 2003 Server Help and Support Center.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.