Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Management of Security Updates in the Windows 2000 Environment

Diligence in the timely deployment of security updates is necessary as part of any effective security program. This paper will address the following areas: Mitigating some risks by initially deploying a secure base configuration, Learning of newly discovered vulnerabilities, Getting the security updates, Testing the security updates in a non-production environment, Scanning production systems for patch installation status, Deploying the security updates and Management policy. While the focus of this paper will be on th...

Copyright SANS Institute
Author Retains Full Rights

AD

James Cebula
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b – Option 1
Management of Security Updates in the Windows 2000 Environment
February 26, 2003

ABSTRACT

Diligence in the timely deployment of security updates is necessary as part of any effective security program. This paper will address the following areas:

- Mitigating some risks by initially deploying a secure base configuration
- Learning of newly discovered vulnerabilities
- Getting the security updates
- Testing the security updates in a non-production environment
- Scanning production systems for patch installation status
- Deploying the security updates
- Management policy

While the focus of this paper will be on the enterprise or corporate computing environment, some issues affecting the home or small business user will be highlighted as well. Also, the scope of this paper is limited to the Microsoft Windows 2000 server and Windows 2000/XP desktop operating systems, widely deployed Microsoft server applications such as SQL Server and Internet Information Services (IIS) Server, and key desktop applications such as Internet Explorer and the Office productivity suite. Although non-Microsoft operating systems and applications are not discussed here, proper management of security updates for these products is equally as important to the overall effectiveness of the security program.

SECURING THE INITIAL DEPLOYMENT

The first and most important step that can be taken toward securing an organization's computing environment is to deploy systems in a secure state initially. This statement may seem unnecessary, but in fact many systems (particularly Microsoft products) by default install in an open configuration where many features are enabled and not secured. To mitigate vulnerabilities, steps need to be taken to disable features that will not be in use and to secure various settings and permissions. This needs to be done before considering a strategy for management of updates and prior to placing the systems into production. Microsoft has stated that enhancing the security of default installs is a corporate goal (Refs. 1 and 2), but in reality they are not there yet.

Fortunately, a number of tools and guides are available from Microsoft and others to facilitate the task of establishing a secure base configuration. Security settings in Windows 2000/XP are managed through group policy objects that are either applied locally at the machine or are enforced through Active Directory (AD) for machines belonging to an AD domain. Collections of security settings

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

are defined in template (.inf) files. The Microsoft Security Configuration and Analysis tool (Ref. 3) allows an administrator to quickly compare the settings in a template against the actual settings on a machine and examine the differences. Windows 2000 ships with a number of templates for workstations, member servers, and domain controllers. Three versions of the templates are available allowing the user to establish basic, secure, or highly secure settings. Microsoft has also developed and documented an additional set of templates based on a modified version of the highly secure templates provided with Windows 2000 (Ref. 4). The referenced documents provide instructions on how to implement the settings defined in the templates, either locally or through AD.

The Center for Internet Security (CIS), in collaboration with the SANS Institute, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the National Institute of Standards and Technology (NIST), and the General Services Administration (GSA), has developed a set of consensus baseline security templates for Windows 2000 (Ref. 5). Two levels of consensus templates are provided. The Level 1 templates provide a minimum acceptable level of security. The Level 2 templates are available for both Windows 2000 Professional and Server and are known as the Gold Standard. These provide a step increase in the level of security and have been determined by the consortium of organizations listed above to represent a best practice. In fact, it has been estimated that about 85% of successful computer system attacks could have been prevented if the systems had been secured using the Gold Standard (Ref. 6).

NSA has provided additional guides and templates (Ref. 7) that go beyond the scope of the Gold Standard guides by covering Windows XP and Windows 2000 Domain Controllers. NSA also provides extensive guide documents to accompany the templates. For Windows 2000 server, the guides not only cover the operating system, but also discuss hardening specific features such as DNS, DHCP, Kerberos, and Encrypting Fie System (Ref. 8). In addition to NSA, the Computer Incident Advisory Capability (CIAC), operated by the Lawrence Livermore National Laboratory, provides configuration guides and templates for use by the Department of Energy (DOE) (Ref. 9).

As shown above, there are a number of tools and pre-defined templates available to enable varying levels of security to be quickly established on an organization's systems. Unfortunately, there is no one-size-fits-all solution here. For example, disabling certain services may cause applications used by the organization to break. The best practice would be to proceed as follows. First, review several of the templates and their documentation. Next, make some reasonable decisions about what changes need to be made to suit the organization's needs. Then, test and document the settings. Finally, establish the revised template as the baseline security model for the organization.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

LEARNING OF NEWLY DISCOVERED VULNERABILITIES

Deployment of an initially secure configuration, as described in the previous section, is an excellent first step toward a secure computing environment, but it is only the beginning. The newly-deployed secure systems will not stay secure for long, since new vulnerabilities with Microsoft products are discovered and publicized at a rapid pace. A quick check of the Microsoft TechNet archives of security bulletins (Ref. 10) indicates that as of this writing, Microsoft has already issued 6 security bulletins in 2003. In 2002, 72 bulletins were issued, 60 were issued in 2001, and 100 in 2000. The sheer number of vulnerabilities and the exploits that result when the vulnerabilities are left unpatched have caused considerable bad publicity for Microsoft. In fact, in March 2002 the WORM_GIBE.A virus began propagating on the Internet as an e-mail attachment designed to look like a Microsoft security bulletin (Ref. 11).

Given the statistics above, it's clear that system administration and security personnel are required to stay abreast of the latest vulnerability announcements. The most important step to take here is to subscribe to one of Microsoft's e-mail notification services. Microsoft provides two options for e-mail notification of updates. One is the Microsoft Security Update newsletter (Ref. 12) that is geared toward the home user or someone not interested in the technical details of the vulnerability. The other, and the one recommended for system administration and security practitioners is the Microsoft Security Notification Service (Ref 13). The Security Notification Service provides an e-mail version of the security bulletin that has been digitally signed to help prevent worms as described earlier. The Microsoft security bulletins themselves provide a wealth of information concerning the technical details of the vulnerability, mitigating factors, affected systems, severity ratings, links to the patches, and verification of the patch installation. The bulletins also provide valuable information on the patch dependencies, installation requirements, and links to any relevant knowledge base articles. It is important to note that other security organizations, such as the Computer Emergency Response Team Coordination Center (CERT/CC) located at Carnegie Mellon University, and CIAC often issue their own identification numbers and bulletins covering Microsoft vulnerabilities. However, the CERT and CIAC bulletins often either refer back or directly link to the relevant Microsoft bulletin. Therefore, subscribing to the Microsoft bulletins is generally a good practice for administrators to provide early notification of security issues.

Another excellent source of regularly updated vulnerability information is the SANS/FBI Top 20 list (Ref. 14). The list contains the top 10 vulnerabilities in both Windows and UNIX. For each vulnerability identified, specific detailed steps to mitigate it are provided. The items on the Top 20 list are somewhat different than the items reported in Microsoft Bulletins. Top 20 list vulnerabilities address known weaknesses in the system and are often mitigated by disabling a specific feature or setting, rather then by applying a patch. The Top 20 are also geared

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

toward resolving a small number of critical vulnerabilities that have been shown to cause a large number of exploits.

GETTING THE SECURITY UPDATES

A number of sources are available to obtain the required Microsoft security updates. The first, but least automated method, is by direct download from Microsoft. The Microsoft TechNet archive of security bulletins (Ref. 10) contains a search feature that allows searches by product and service pack level or by Knowledge Base article number. Clicking the link to a specific bulletin will provide further links to download the executable for the desired patch. The executable then needs to be run on each system where it is to be applied. This method of manual download and install is the most time-consuming, but it is the best available in cases such as where the machines are not directly connected to the Internet. However, some guesswork may be required on the part of the user to determine exactly which updates apply to a particular system.

The Microsoft Windows Update website (Ref.15) provides a number of services to obtain and install patches. The website contains a scanning tool that will check single Internet-connected computers to determine what updates are necessary. The site will then allow the user to select from a list of available updates and have them downloaded and installed automatically. There are a number of advantages to this method of updating. First, this site includes all critical updates and service packs, as well as recommended OS and driver updates. The critical updates and service packs are generally those that have a security impact and need to be acted upon promptly. Critical updates are also identified by Microsoft in the security bulletins discussed in the previous section. The recommended updates either fix known non-security related flaws in the OS or add new features to extend the functionality of the system. Driver updates are generally supplied by third-party vendors and have been tested by Microsoft to improve the compatibility between Windows and various peripherals such as video adapters and network interface cards. The Windows Update site provides a convenient source for all of these updates. Secondly, the list of available updates returned by the site is customized based on which updates have been previously installed, and what OS and hardware are present on the machine. This feature eliminates any guesswork needed in the manual download process, discussed above, as to which updates are applicable to a given machine. There are some disadvantages to the Windows Update site as well. First, the site only scans and installs updates on the machine from which it is run. This makes the site a valuable tool for home or small business users with only a small number of systems, but is ineffective and cumbersome in an enterprise computing environment with a large number of machines. In an enterprise managed network, administration and configuration control will quickly become impossible if each user is individually updating their machine from Windows Update. For this reason, a group policy that blocks access to the Windows Update facility is provided by Microsoft and can be deployed to Windows 2000 or XP machines

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

that are managed as part of an AD domain. Second, since the site automatically downloads and installs the updates, the machine must be connected to the Internet. If the machine is not connected to the Internet, or if the user needs to keep a copy of the executable for the update for later use, this method will not work. Third, the user who is downloading and installing the updates must, in most cases, be logged in with local administrative privileges. This may be undesirable or impossible both in the enterprise and home environments. The Microsoft Office Product Updates website (Ref.16) provides similar functionality as Windows Update but covering the Office suite of products. Similar advantages and disadvantages as discussed above for Windows Update also apply for Office Update. It is also important to note that in many corporate or enterprise installations, Office is installed onto the desktops from a central server location known as an admin point. In these types of installations, the correct way to apply updates and service packs is for an administrator to apply the update to the admin point at the server and then re-deploy the application to the workstations (Ref. 17). A user attempting to update his installed copy of Office with patches downloaded from Office Update will actually corrupt his local installation.

The two methods of obtaining updates discussed thus far, direct download and Windows/Office update, are both manual processes that require an administrator or end user to take action to download and install the updates. In Windows XP Microsoft introduced the Automatic Updates service. Automatic Updates was also added to Windows 2000 in Service Pack 3. The Automatic Updates feature allows the user or administrator to configure the computer to automatically check with the Windows Update website for applicable critical updates whenever there is an Internet connection present. A user with administrative privileges on the machine can configure Automatic Updates settings locally, or a system administrator can manage Automatic Updates settings for computers in an AD domain through group policy. When Automatic Updates is enabled, the computer checks for the availability of new critical updates. If a new critical update is available, Automatic Updates can be further configured to take one of three actions: 1) notify the user twice, once to begin the download and again when the download is complete and ready for install, 2) download the update automatically and notify the user only when the download is complete and ready for install, or 3) automatically download and automatically install and reboot if necessary according to a configurable schedule. The downloads are done in the background via another new Windows service called the Background Intelligent Transfer Service (BITS). BITS uses idle bandwidth to “drizzle” the downloaded files to the computer. This ability to automatically download and install critical updates, thus keeping a computer always up-to-date with security patches, is clearly powerful. However, there are some disadvantages. First, Automatic Updates only checks for critical updates to the operating system and applications integral to the OS, e.g. Internet Explorer and Outlook Express. While this is a significant step toward a more secure computing environment, some necessary areas are not covered. For example, service packs, which are sometimes

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

necessary for security fixes, are not discovered or deployed with Automatic Updates. Updates for server applications and Office are not covered, either. Second, Automatic Updates will only work correctly on machines connected to the Internet, similar to Windows Update. Third, in the corporate environment, having a large number of machines connect to the Internet independently to obtain updates would use a significant amount of external bandwidth.

As discussed above, Automatic Updates improves upon Windows Update by providing some automation functionality for critical updates but still has some disadvantages in the corporate environment. The Software Update Services (SUS) Server product is available as a free download from Microsoft (Ref. 18) to address some of these shortcomings. SUS Server essentially allows systems administrators to establish an internal Windows Update server and then use the clients' Automatic Updates functionality to download and install critical updates from the internal server rather than from the Internet. The Automatic updates settings necessary to direct the clients to update from the internal SUS server rather than from the Internet are managed through Group Policy. Reference 18 also provides a link to a detailed white paper covering various implementation options for SUS Server. The SUS Server is configured to download updates from Microsoft via the Internet, and then make the list of updates available to the client machines on the internal network. One important aspect of SUS Server is the ability to create a distributed SUS deployment within the organization. One Internet-connected SUS server can be used to replicate the collection of security updates to other non-Internet-connected SUS servers, thus distributing the load in large organizations. Perhaps the most significant feature of SUS server is that it provides several options on how to handle distribution of new updates that it has downloaded from Microsoft. The most significant choice is the option to hold new updates until they are approved by an administrator for distribution. This provides a hold point to allow administrators to test the updates before deploying them on production devices. Testing will be discussed in more detail in the next section. This "hold for approval" feature is not provided by Windows Update and Automatic Updates.

Other products are also available for obtaining security patches. These include the Software Update Services Feature Pack for Systems Management Server (SMS) by Microsoft, and HFNetChk Pro by Shavlik. While these products can be used as a mechanism to download security updates, their real added value is in scanning for patch installation status and deployment of patches. These products will be discussed in more detail in later sections of this paper.

TESTING THE SECURITY UPDATES IN A NON-PRODUCTION ENVIRONMENT

The importance of performing some level of testing on updates prior to deploying them on a production system cannot be over-emphasized. However, development of a prototypical test environment can be a very expensive and time

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

consuming undertaking. Microsoft provides a detailed guidance on setting up and managing a test lab for Windows 2000 as part of the Windows 2000 Server Deployment Guide (Ref. 19). This guidance essentially advocates having a test lab that fully replicates the hardware, software, and services available on the production network. This would include similar hardware for servers, software licenses for all needed products (including third-party products that need to interoperate with the Microsoft products), all network services such as DNS and DHCP, and prototypical client workstations and applications. Depending on the size, the Microsoft guidance also recommends employing additional personnel just to manage the test lab on a full-time basis. Part of Microsoft's rationale to justify this investment is that the test lab should be set up during the initial deployment of or upgrade to Windows 2000 and then left in place as a permanent lab to test ongoing updates, patches, and service packs. Obviously, following this guidance would represent a significant investment of both financial and manpower resources for any organization. However, if an organization determines that some or all of its IT services are mission critical, this level of investment in testing may be justified and an extraordinary level of effort may need to be applied to pre-production testing of updates prior to deployment. In the case of security updates, an assessment needs to be made as to whether the organization's systems are actually vulnerable to the problem corrected by the update. The circumstances surrounding the security update, such as whether the vulnerability is currently being exploited, need to be well understood. In cases where an organization is indeed vulnerable to an exploit, the updates will need to be deployed on an urgent basis. In this case, the amount of time allocated for testing may need to be reduced, or a decision may need to be taken to shut down certain features or services until the patches can be tested and applied.

A number of universities have published the details of their Windows 2000 test lab specifications and experiences. These include Portland State University (Ref. 20), Virginia Tech University (Ref. 21), and the University of California at San Francisco (Ref. 22). Reviewing the published details of setups is instructive, and it appears that in most cases these Universities plan to maintain the test labs as permanent facilities in keeping with Microsoft's recommendations.

Clearly, the extent of required testing of updates and the appropriate level of investment in a test facility is a business decision. It will require input from the organization's management, security, technology, and possibly legal communities. It is important that whatever level of testing is decided upon is documented in a change control procedure. Additionally, the baseline or initial state of the production system configuration should be well documented. The change control procedure should then define what documentation is required to describe the before and after state of each change. The results of any testing done on the change in the test environment should also be documented. This can become valuable for later troubleshooting. For example, a particular patch may only be able to be applied to systems at a certain service pack level or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

higher. Machines in the test environment were all at the correct service pack and the patch testing was successful. However, a production machine may, for whatever reason, not be at the correct service pack level for the update. This machine could then be highlighted for special handling, since the testing documentation has provided awareness that older service pack was not part of the tested configuration.

SCANNING PRODUCTION SYSTEMS FOR PATCH INSTALLATION STATUS

Another important aspect of update management is the capability to scan systems to determine whether a patch needs to be applied, and if an install was successful. A number of free and commercial tools are available to accomplish this. One simple yet powerful tool is the command line utility HFNetChk.exe developed for Microsoft by Shavlik Technologies. This tool is available as a free download from both Microsoft and Shavlik (Ref. 23) and is essential for both system administration and security personnel. HFNetChk relies on an XML file that defines the current list of updates and service packs that Microsoft has released. If the machine running the tool is connected to the Internet, the tool will download and use the current version of the XML file on the fly. In order to scan machines not connected to the Internet, the XML file can be downloaded manually and identified using command line switches when HFNetChk is executed. HFNetChk can scan machines or machine groups remotely, can produce various formats of reports, and also scans for updates to a large number or Microsoft operating systems and applications, excluding Office. According to Shavlik,

> "You can use HFNetChk to assess patch status for the Windows NT 4.0, Windows NT Terminal Server, Windows 2000, Windows XP operating systems, as well as hotfixes and service packs for IIS 4.0, IIS 5.0, SQL Server 7.0, SQL Server 2000 (including MSDE), Exchange Server 5.5, Exchange Server 2000, Windows Media Player, Front Page Server Extensions, Microsoft Java Virtual Machine, Microsoft Data Access Components (MDAC), and Internet Explorer 5.01 or later." (Ref. 23)

Because HFNetChk is command-line based, it can easily be set up to run as a Windows scheduled task to scan a group of machines on a regular basis and generate reports to be reviewed by administrators to determine patch compliance.

The Microsoft Baseline Security Analyzer (MBSA) version 1.1 is available as a free download from Microsoft (Ref. 24). MBSA builds upon, and adds a graphical interface to HFNetChk. MBSA also checks a number of windows security settings such as local account password policies, whether the file system is NTFS, and Internet Explorer security zones.

The Center for Internet Security (CIS) scoring tool is also available for free download (Ref. 5). Like MBSA, the CIS tool also uses the HFNetChk XML file to scan for the presence or absence of service packs and hotfixes. An XML formatted report is generated showing the patch status. The CIS tool

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

allows for other security settings on the machine to be checked against a user selected template file. The tool then provides a score in each area, which is rolled up into an overall score for the machine.

Visual Basic Scripts (VBScripts) are also available to query the hotfix status of a particular machine or group of machines (Ref. 25). The script attaches to the Windows Management Instrumentation (WMI) provider on the machine and reports several properties about each installed hotfix. The core of the script can be used within a larger script that connects to a group of machines and generates consolidated reports. This script reports on patches that are already installed, and does not report on updates that need to be installed. As such, this script is valuable for determining if the installation of a particular update was successful. It is not as effective as the other tools discussed above for determining if required patches are missing.

DEPLOYING THE SECURITY UPDATES

There are a number of methods available to deploy the security updates. Several of these methods make use of tools and processes discussed previously for downloading and scanning. Directly installing the patch from an executable file that was manually downloaded is a reliable deployment method, and may be the only option available for systems that are not connected to the Internet. However, it is not practical in large distributed networks since it would require a user with administrative privileges to log in locally at each machine. The Windows Update website and the Automatic Updates service in Windows 2000 SP3 /XP discussed previously are both good deployment mechanisms for home users or for small networks where each machine has a connection to the Internet. For corporate networks of a moderate size where implementation of one of the more advanced deployment infrastructures discussed below is not feasible, the SUS server coupled with the Automatic Updates client is a reliable way to deploy critical updates. SUS is, of course, subject to the disadvantages discussed previously, namely that it does not deploy service packs or Office updates.

For computers that are managed within an AD domain, the software assignment features of Group Policy can be utilized to deploy service packs and security updates. This feature can be used to install any software that is distributed as a Microsoft Installer (MSI) package. Microsoft is now including the MSI package with the OS service packs. In these cases, deployment can be handled directly by assigning the service pack to machines through a Group Policy object. In the case of application service packs or hotfixes, a tool such as WinInstall by Veritas can be used to take before and after snapshots of a machine as the patch is installed on a test system. WinInstall then generates an MSI package from the differences in the system caused by the install. This snapshot procedure has the disadvantages of being sensitive to slight differences in configuration between

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the test system and the target systems, and it can be difficult to troubleshoot in the case of failed installs.

HFNetChk Pro is a commercial tool published by Shavlik (Ref. 26) that uses the HFNetChk functionality to scan machines for patch and service pack installation but adds the powerful ability to download the patches from Microsoft into a repository and then deploy them to the clients. This tool effectively combines the functions of scanning machines to determine the patches that are needed, downloading the patches, and deploying them. Support for a wide range of Microsoft products is built into HFNetChk pro. Support for additional products, notably Office and Outlook, is scheduled to be available in early 2003.

Microsoft states that its Systems Management Server (SMS) product is the method of choice for patch deployment in medium to large sized organizations (Ref. 27). SMS is a complex package for software distribution and management and a discussion of the details of its operation is beyond the scope of this paper. However, administrators and security personnel should be aware of the Software Update Services Feature Pack for SMS 2.0 that is available for free download from Microsoft (Ref. 28). The SUS Feature Pack for SMS adds the following functionality to the core features of SMS 2.0: a security update inventory tool, an Office inventory tool for updates, a wizard-based tool for distribution of software updates, and a web-based reporting tool. The Feature Pack also supports updates for the OS, major applications, and Office. Much of the functionality that was added onto SMS 2.0 by the SUS Feature Pack is built into SMS 2003, the next version of SMS that is currently released in beta. If an SMS infrastructure is already in place within the organization then the Feature Pack is a very effective tool for management of patches and updates. Also, even if SMS is not installed in an organization with a sizable network, the Software Update features of the Feature Pack could be of sufficient value to drive an implementation of SMS.

MANAGEMENT POLICY

The preceding sections have discussed some of the technical issues associated with management of security updates. In addition to technical issues, the organization needs to be aware of and address certain policy issues. In this area, however, there are no hard and fast rules. Each organization needs to evaluate its business needs and determine what policies are appropriate. Development of a policy will almost certainly need to be a collaborative process involving IT, security, management, legal, and possibly customers. Some policy issues that should be considered are highlighted in the following discussion.

One area that should be addressed and defined in a policy is roles and responsibilities. For example, will a dedicated security group be responsible for locating and directing action on the patches, or will the system administrators have this responsibility. Another is the need for a policy on who has the responsibility to determine if a particular patch is deemed to be critical, and once

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

this determination is made, are there different (or any) guidelines covering how much time is allotted for testing and deployment. In addition, there may be specific external requirements (regulatory, governmental, customer, etc.) that need to be addressed. As just one example, organizations in the health care industry would need to address the security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The organization's policies will also need to address the types of software in use. It may be appropriate to have a policy requiring software that is no longer vendor supported not be used in the organization. In the case of Microsoft products, there are security implications with using unsupported versions, since Microsoft no longer provides security-related hotfixes once a product has reached end-of-life (Ref. 29). If the organization is in the software development business, such an end-of-life policy may not be feasible since the older OS versions may be needed to provide ongoing support for the company's products. Also, a software development company may find itself in the position of discovering vulnerabilities in another vendor's products or operating systems. Policy on how to handle these discoveries will need to be decided upon by management and documented. The organization will likely want to enforce a policy of quietly disclosing these discoveries to the vendor to allow verification of the problem and to allow the affected vendor time to produce a patch.

Guidance on and examples of policies are available on the Internet from a variety of sources such as RFC 2196, the SANS Institute (Ref. 30), and Texas A&M University (Ref. 31). Similar to the discussion earlier in this paper regarding Windows security templates, the best practice here would be for the organization to use the guidance available as reference material, then critically review the organizations' needs and develop a policy based on that review.

SUMMARY AND CONCLUSION

Effective management of security updates for all deployed operating systems and applications is a necessary element in any organization's security program. In most organizations, this will include at least some deployments of Microsoft operating systems and applications. This paper has provided the framework for a process that can be utilized by system administration personnel and by information security officers to manage the deployment of security updates. The following general steps in the process were discussed:

- Mitigating some risks by initially deploying a secure base configuration
- Learning of newly discovered vulnerabilities
- Getting the security updates
- Testing the security updates in a non-production environment
- Scanning production systems for patch installation status
- Deploying the security updates
- Management policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In each of these areas, resources and techniques specific to the Microsoft Windows 2000 environment were presented. Although the focus of this paper was Microsoft products, a similar process could be followed for other operating systems and applications, and is in fact a fertile area for future papers and research.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

1. Gates, Bill. "Security in a Connected World." January 23, 2003. http://www.microsoft.com/mscorp/execmail/ (February 17, 2003).
2. Microsoft Corporation. "Building a Secure Platform for Trustworthy Computing – White Paper." December 2002. http://www.microsoft.com/security/download/secure_platform.doc (February 17, 2003).
3. Microsoft Corporation. "HOW TO: Analyze System Security in Windows 2000." Microsoft Knowledge Base. KB313203. October 26, 2002. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313203&sd=tech (February 17, 2003).
4. Microsoft Corporation. "Security Operations Guide for Windows 2000 Server." March 14, 2002. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp (February 17, 2003).
5. Center for Internet Security. "Benchmarks and Scoring Tool for Windows 2000 and Windows NT." December 2002. http://www.cisecurity.org/bench_win2000.html (February 18, 2003).
6. SANS Institute. "Securing Windows 2000 – The Gold Standard." December 2002. http://www.sans.org/win2k/win2k.php (February 18, 2003).
7. National Security Agency. "Security Recommendation Guides." November 25, 2002. http://nsa2.www.conxion.com/index.html (February 18, 2003).
8. National Security Agency. "Security Recommendation Guides – Windows 2000 Guides." October 17, 2002. http://nsa2.www.conxion.com/win2k/download.htm (February 18, 2003).
9. Orvis, William J., Kathryn Call, and John Dias. "Connecting to the Internet Securely; Windows 2000." CIAC-2321. March 2002. http://www.ciac.org/ciac/documents/CIAC-2321_Connecting_to_the_Internet_Securely_Windows_2000.pdf (February 18, 2003).
10. Microsoft Corporation. "Hotfix and Security Bulletin Service." http://www.microsoft.com/technet/treeview/?url=/technet/security/current.asp?frame=true (February 18, 2003).
11. Olavsrud, Thor. "Beware of Microsoft Security Updates." March 6, 2002. http://www.internetnews.com/dev-news/article.php/10_986251 (February 18, 2003).
12. Microsoft Corporation. "Microsoft Security Update." http://register.microsoft.com/subscription/subscribeme.asp?id=166 (February 18, 2003).
13. Microsoft Corporation. "Product Security Notification." October 2002. http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/notify.asp (February 18, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

14. SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities." Version 3.21. October 17, 2002. http://www.sans.org/top20/ (February 18, 2003).
15. Microsoft Corporation. "Microsoft Windows Update." http://v4.windowsupdate.microsoft.com/en/default.asp (February 23, 2003).
16. Microsoft Corporation. "Office Product Updates." http://office.microsoft.com/ProductUpdates/default.aspx (February 23, 2003).
17. Microsoft Corporation. "OFF2000: How to Install an Update to Administrative Installations." Knowledge Base Article 304125. August 6, 2002. http://support.microsoft.com/default.aspx?scid=kb;en-us;304165 (February 23, 2003).
18. Microsoft Corporation. "Software Update Services Server 1.0 with Service Pack 1." January 31, 2003. http://www.microsoft.com/downloads/details.aspx?FamilyId=A7AA96E4-6E41-4F54-972C-AE66A4E4BF6C&displaylang=en (February 23, 2003).
19. Microsoft Corporation. "Windows 2000 Server Deployment Guide – Chapter 4 – Building a Windows 2000 Test Lab." http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/deploy/part1/chapt-4.asp (February 23, 2003).
20. Portland State University, Office of Information Technology. "Windows 2000 Test Environment." May 2, 2002. http://www.oit.pdx.edu/netadmin/windows/test/ (February 23, 2003).
21. Virginia Tech, Information and Systems Computing. "VT AIS Windows 2000 Pilot Project – Test Lab Environment." May 15, 2002. http://www.it.vt.edu/organization/isc/w2kpilot/testlab.htm?format=W2Kweb (February 23, 2003).
22. University of California at San Francisco. "The Windows 2000 Project Test Labs." May 6, 2001. http://www.ucsf.edu/its/windows2000/testing.html (February 23, 2003).
23. Shavlik Technologies. "HFNetChk.exe." November 20, 2002. http://www.shavlik.com/pHFNetChkExe.aspx (February 24, 2003).
24. Microsoft Corporation. "Microsoft Baseline Security Analyzer." Version 1.1. December 2, 2002. http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (February 24, 2003).
25. Microsoft Corporation. "System Administration Scripting Guide - Enumerate Installed Hot Fixes." http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/ScrCM15.asp (February 25, 2003).
26. Shavlik Technologies. "HFNetChk Pro." http://www.shavlik.com/pHFNetChkPro.aspx (February 24, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

27. Microsoft Corporation. "Patch Management Using Microsoft Systems Management Server." 2002. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/msm/swdist/pmsmsog.asp (February 25, 2003).
28. Microsoft Corporation. "SMS Software Update Services Feature Pack." December 18, 2002. http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/default.asp (February 25, 2003).
29. Microsoft Corporation. «Windows Desktop Product Life Cycle Support and Availability Policies or Business." October 15, 2002. http://www.microsoft.com/windows/lifecycle/desktop/business/default.mspx (February 25, 2003).
30. SANS Institute. "What do I put in a Security Policy?" October 16, 2002. http://www.secinf.net/policy_and_standards/What_Do_I_Put_in_a_Security_Policy_.html (February 25, 2003).
31. Texas A&M University. "24.99.99.M1 – Security of Electronic Information Resources." May 27, 2002. http://rules.tamu.edu/urules/200/249999M1.htm (February 25, 2003).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 2nd, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS FOR508 Hamburg in German	Hamburg, DE	May 09, 2016 - May 14, 2016	Live Event
SANS Melbourne 2016	Melbourne, AU	May 16, 2016 - May 21, 2016	Live Event
Beta 2 Cincinnati - ICS456	Covington, KYUS	May 16, 2016 - May 20, 2016	Live Event
Security Operations Center Summit & Training	Crystal City, VAUS	May 19, 2016 - May 26, 2016	Live Event
SANS SEC401 Luxembourg en francais	Luxembourg, LU	May 30, 2016 - Jun 04, 2016	Live Event
SANSFIRE 2016	Washington, DCUS	Jun 11, 2016 - Jun 18, 2016	Live Event
SANS Philippines 2016	Manila, PH	Jun 20, 2016 - Jun 25, 2016	Live Event
SANS Pen Test Berlin 2016	Berlin, DE	Jun 20, 2016 - Jun 25, 2016	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 23, 2016 - Jun 30, 2016	Live Event
SANS Salt Lake City 2016	Salt Lake City, UTUS	Jun 27, 2016 - Jul 02, 2016	Live Event
SANS Cyber Defence Canberra 2016	Canberra, AU	Jun 27, 2016 - Jul 09, 2016	Live Event
MGT433 at SANS London Summer 2016	London, GB	Jul 07, 2016 - Jul 08, 2016	Live Event
SANS London Summer 2016	London, GB	Jul 09, 2016 - Jul 18, 2016	Live Event
SANS Rocky Mountain 2016	Denver, COUS	Jul 11, 2016 - Jul 16, 2016	Live Event
SANS Minneapolis 2016	Minneapolis, MNUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS San Antonio 2016	San Antonio, TXUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS Delhi 2016	Delhi, IN	Jul 18, 2016 - Jul 30, 2016	Live Event
Industrial Control Systems Security Training	Houston, TXUS	Jul 25, 2016 - Jul 30, 2016	Live Event
SANS San Jose 2016	San Jose, CAUS	Jul 25, 2016 - Jul 30, 2016	Live Event
Security Awareness Summit & Training	San Francisco, CAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Prague 2016	OnlineCZ	May 09, 2016 - May 14, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced