realtimepublishers.com™

The Administrator Shortcut Guide™ To

Patch Management

NEW BOUNDARY
TECHNOLOGIES

Rod Trent

Introduction

By Sean Daily, Series Editor

Welcome to *The Administrator Shortcut Guide to Patch Management!*

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as New Boundary Technologies who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it *won't* cost you $30 to $80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, New Boundary Technologies has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my *raison d'être* to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Copyright Statement

© 2004 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 1: Why is Patch Management Important?

For the majority of companies, security has become the top issue for planning and implementing technologies, and effective security in today's environment goes well beyond simply running antivirus applications and installing firewalls. Total security also encompasses user and IT staff education and training. And key to gaining overall security, as we will explore in this guide, is patch management.

To lay the foundation for a more detailed discussion of patch management in later chapters, this chapter provides an overview of the barriers to implementing and maintaining a secure environment, the state of security in the computing world, and potential vulnerabilities in any organization. This groundwork will enable us to explore the crucial idea behind patch management: Patch management is not a one time operation but a series of ongoing steps and processes to bring the environment within the most current secure specifications. Let's begin with a focus on overall security, which will illustrate and emphasize the importance of patch management in a successful security strategy.

The Security Landscape

It's an insecure world. Each day we read about new threats to computer security, and whether these threats result from operating system (OS) vulnerabilities or holes in application security, it is difficult to keep up with the number of patches that are constantly being released. As time has progressed, new types of threats have surfaced, making each area of the computer vulnerable to a wide range of exploits. The following list highlights some of the top vulnerability categories:

- OS vulnerabilities—OS vulnerabilities, although not the most common, tend to gain the most media coverage. OS vulnerabilities are one of the security aspects targeted by patch management.
- Application vulnerabilities—In addition to the OS being vulnerable to exploits, the applications that run on the OS can also require patching. Some prominent applications for which patches are regularly released include Microsoft Office, Microsoft SQL Server, and Microsoft Exchange Server as well as third-party Independent Software Vendor (ISV) software products.
- Viruses—A virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector, or document. Viruses can be transmitted as attachments to an email message or in a downloaded file, or be present on a diskette or CD-ROM. Over the past year, antivirus software application vendors have performed double-duty by providing, through their updating mechanisms, fixes to exploits that ultimately should be dealt with through patch management.

-

> There are three main classes of viruses. The following list provides definitions of each:
>
> **File infectors—**Some file infector viruses attach themselves to program files, usually selected .COM, DLL, or .EXE files. Some can infect any program or process for which execution is requested, including .SYS, .OVL, .PRG, and .MNU files. When the program is loaded, the virus is loaded as well. A virus can even bind itself to the OS shell.
>
> **System or boot-record infectors—**These viruses infect executable code found in certain system areas on a disk. The viruses attach to the DOS boot sector on diskettes or the Master Boot Record (MBR) on hard disks. A typical scenario is to receive a diskette from an innocent source that contains a boot disk virus.
>
> **Macro viruses—**These viruses are among the most common and they tend to do the least damage. Macro viruses infect Microsoft Word and typically insert unwanted words or phrases.

- Worms—A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an OS that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. Worms most commonly exploit known software flaws or vulnerabilities.
- Spam—Spam is unsolicited email. From the sender's point-of-view, spam is a form of bulk mail, often to a list obtained from a spambot or by companies that specialize in creating email distribution lists. To the receiver, it usually seems like junk email. It's roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message because everyone shares the cost of maintaining the Internet. Spam can also carry viruses that, upon viewing, infect a system.
- Spyware—Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.
- Adware—Adware is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to lower the cost for the user.

Exploits are growing not only in number but also in complexity. For example, the recent Sasser worm exploited a Microsoft Windows vulnerability, and it required no user interaction to do damage. In other words, the user did not have to click an email attachment or run a virus-infected program. Granted, there are many factors outside of the control of companies that contribute to the spreading of worms and viruses (for example, home users), but if companies had had an effective patch management solution in place, Sasser would not have been as successful in replicating itself across their networks because the patch to plug the exploit Sasser utilized was available several weeks prior to the worm's release. In the same respect, it is alarming how the patch-to-exploit time is decreasing. In other words, when a patch is made available by a vendor, virus writers are developing and releasing their terrorist code sooner than ever.

Even with the patch-to-exploit time decreasing substantially, many virus and worm writers still attempt to develop viruses based on old exploits. These viruses and worms are targeting those uninformed or uneducated end users. Even in this day and age, where computers are everywhere and in use every minute of the day, there are still those computer users that have failed to receive the message that computer security responsibility resides with them first.

To get a better understanding of the overall landscape of computer security, it is helpful to know how times have changed. The Computer Emergency Response Team (CERT) maintains statistics about past reported incidents and vulnerabilities. Table 1.1 illustrates that the number of reported incidents and vulnerabilities has steadily increased.

Year	Reported Incidents	Reported Vulnerabilities
2000	21, 756	1,090
2001	52, 658	2,437
2002	82,094	4,129
2003	137,529	3,784

Table 1.1: Reported incidents and vulnerabilities by year. (Source: http://www.cert.org/stats/cert_stats.html.)

> 📖 For more information about CERT, see the resource box at the end of this chapter.

Types of Vulnerabilities

When you think about vulnerabilities and what you can do to minimize your organization's exposure, it is helpful to categorize the possibilities so that you can plan and implement security based on the assigned category:

- Administrative
- Product
- Physical

If you are part of a large company, each category of vulnerability will generally be handled by different teams or individuals. The following sections describe these categories of vulnerabilities and provide factors to help identify the most appropriate category when assigning responsibilities for each.

✎ Of these three vulnerability categories, the product category most directly affects patch management.

Administrative Vulnerabilities

When an administrator fails to observe administrative best practices—for example, by using a weak password or logging on to an account that has more user rights than are necessary to perform a specific task—an administrative vulnerability is introduced. An administrative vulnerability might be the most telling shortcoming in respect to your company's security policies and practices. If an administrator doesn't use proper techniques for securing the environment from an administrative level, there is a good chance that the administrator isn't knowledgeable enough to provide security for the other vulnerability types.

An Administrative Best Practice: Renaming Important Accounts

When attackers try to gain access to your company's network, the Administrator and Guest accounts are the first point of attack: They try to gain access by using methods to hack the passwords associated with these accounts. As a security measure against such attacks, an administrative best practice is to rename or disable the Administrator and Guest accounts for your Windows domain, and create a new Administrator-equivalent account that is used for administrative tasks. The following procedure outlines how to rename the Administrator and Guest accounts in your organization. Consider adding this change to the image that you use to deploy desktops in your company as well as employing this procedure on the Windows domain.

To rename the Administrator and Guest accounts, start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in. In the console tree, right-click your domain or the organizational unit (OU) that contains the Group Policy that you want, then click Properties. Select the Group Policy tab, select the desired Group Policy Object (GPO), then click Edit.

Next, expand Computer Configuration, Windows Settings, Security Settings, and Local Policies, then click Security Options. In the right pane of the Group Policy snap-in, double-click *Rename administrator account*. Select the *Define this policy setting* check box, then type the name to which you want to rename the Administrator account, and click OK.

Next, double-click *Rename guest account*, then select the *Define this policy setting* check box, and provide the name to which you want to rename the guest account. Click OK, then quit the Group Policy snap-in. Finally, click OK, then quit the Active Directory Users and Computers snap-in.

Product Vulnerabilities

Through a default software installation, an OS or application software is installed using all the default settings provided by the programmers. Performing a default software installation on computers with sensitive data is not a good practice, especially when the chosen software is likely to be used by many people, such as on a public access computer or Web server. The reason is that, especially with earlier OSs and software, the default settings do not usually result in a secure system.

Over the past year, vendors have stepped up progress to change the way OSs and applications are installed so that a system installed with the default settings for new installations will be secure by default. If you want to enable a feature or service, you will need to know of any risks associated with turning the feature or service on.

All too frequently, patches for known security problems are not applied during a default installation. Granted, as software vendors write increasingly complex code, it becomes more difficult for them to keep up with the production of the necessary patches. Thus, server and systems administrators *must* make the effort to keep their systems patched.

Patching provides vendor-developed solutions to found or known vulnerabilities in their products. The following list highlights common product vulnerabilities:

- Buffer overrun—Buffer overrun is a condition that results from adding more information to a buffer than it was designed to hold. An attacker might exploit this vulnerability to take over a system by inserting code of his or her choice into a program's execution file after an overrun of memory in the buffer takes place. A buffer is a region of memory reserved for use as an intermediate repository in which data is temporarily held before it is transferred between two locations or devices.
- Elevation of privileges—An elevation of privileges is the process by which a user misleads a system to grant unauthorized rights, usually for the purpose of compromising or destroying the system. This vulnerability can be the result of a buffer overrun or an integer overflow attack.
- Denial of Service (DoS) attack—A Dos attack is a computerized assault launched by an attacker to overload or halt a network service, such as a Web server or a file server. For example, an attack might cause the server to become so busy attempting to respond that it ignores legitimate requests for connections.

To protect the installed computer base, the goal is to bring each computer to the most current security specification through proactive patching. There are strategies that you can use in combination with patching that can minimize the exposure to dangerous security flaws. These strategies offer an important educational opportunity for providing security knowledge throughout the organization.

Never Assume that a Default Software Installation Is Secure

Software vendors tend to make their installation programs as generic as possible, focusing on ease of use rather than good security practices. There are four separate vulnerabilities you should be aware of when installing an OS or application:

- Default services installed (mainly applies to OSs; however, you should always check what services are installed with applications as well as the ports that the applications use to communicate across the network)
- Flaws in code
- Sample scripts and templates
- Default accounts and passwords

If you're looking to disable unnecessary services on your Windows servers for security purposes, the following list highlights services you should *never* disable. Disabling any of the services in the list will cause key server and network processes to stop functioning. These services are required for a member server to function within a domain structure:

- COM+ Event System—Permits management of component services
- Dynamic Host Configuration Protocol (DHCP) Client—Is required to update records in dynamic Domain Name System (DNS)
- Distributed Link Tracking Client—Is used to maintain links on NTFS volumes
- DNS Client—Permits resolution of DNS names
- Event Logs—Permits event log messages to be viewed in the event logs
- Logical Disk Manager—Is required to make sure dynamic disk information is updates
- Logical Disk Manager Administration Service—Is required to perform disk administration
- Net Logon—Is required for domain participation
- Network Connections—Is required for network communication
- Performance Logs and Alerts—Collects performance data for the computer, then writes the performance data to a log or triggers alerts
- Plug and Play (PnP)—Is required for Windows 2000 (Win2K) to identify and use system hardware
- Protected Storage—Is required to protect sensitive data such as private keys
- Remote Procedure Call (RPC)—Is required for internal processes in Win2K
- Remote Registry Service—Is required for the Hfnetchk utility
- Security Accounts Manager (SAM)—Stores account information for local security accounts
- Server—Is required for the Hfnetchk utility

- System Event Notification—Is required to record entries in the event logs
- TCP/IP NetBIOS Helper Service—Is required for software distribution in Group Policy; can be used to distribute patches
- Windows Management Instrumentation (WMI) Driver Extensions—Is required to implement performance alerts by using the Performance Logs and Alerts service.
- Windows Time—Is required for Kerberos authentication to function consistently
- WorkStation—Is required to participate in a domain

> There might be additional services in your environment that need to run for functional or security purposes that should also never be disabled. It is highly recommended that you test for proper functionality of each service before you start shutting them off. For example, due to a recent vulnerability, some self-noted "experts" recommended disabling the DCOM service. Disabling the DCOM service caused critical business applications to stop functioning.

Always Require Strong Authentication

The goal of an authentication system is to verify who a user is, which then determines what data is available to that user. Each company's security level needs will be different, but consider including the following in your password policy: Strong passwords are at least eight characters, do not contain all or part of the user's account name, and contain at least three of the four following categories of characters:

- Uppercase letters
- Lowercase letters
- Base 10 digits
- Symbols found on the keyboard (such as !, @, and #)

Always Perform and Verify Backups

In an emergency in which one or more of your servers has gone down and must be restored, having reliable backups of your data is critical—especially if you can't afford to be down for very long. If backups are not made daily or at an interval acceptable to your library, you will not be able to quickly recover (or recover at all) from data loss. You should create backup procedures that state which data must be backed up, when backups must be made, how they must be tested, where the backup media is stored, and how restores are performed.

> If you're using Windows XP, you can also rely on the Restore Point technology for backups. For more information about this technology, see the Microsoft article "Use System Restore to Undo Changes if Problems Occur" at http://www.microsoft.com/windowsxp/pro/using/howto/gethelp/systemrestore.asp.

📖 In addition to backing up the servers, consider backing up the domain infrastructure. Microsoft provides a detailed process for doing so in the article “Domain Infrastructure Backup and Recovery” at http://www.microsoft.com/technet/security/guidance/secmod210.mspx, and in the article “Member Server Baseline Backup and Recovery” at http://www.microsoft.com/technet/security/guidance/secmod211.mspx.

Close All Unused Ports

As open windows to a computer, ports wait for a particular kind of communication. The more ports your servers have open, the easier it is for attackers to connect to that server. In addition, the types of ports your server has open can give away a lot of information about it. One of the first things an attacker will do is monitor your network traffic to try to see which ports are in use. An important security implementation is to restrict which traffic is allowed into your network by allowing only traffic through certain ports on your firewall.

The Netstat Command

You might already be familiar with the Netstat command. What you might not know is that Netstat can be used to determine which Windows XP process is using or blocking TCP/IP ports on your computer. Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, Netstat displays active TCP connections.

As the following list illustrates, Netstat has several parameters (using netstat /? in a command prompt window will display all available command-line parameters):

-a—Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

-e—Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.

-n—Displays active TCP connections; however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

-o—Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.

-p Protocol—Shows connections for the protocol specified by protocol. In this case, protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.

-s—Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.

-r—Displays the contents of the IP routing table. This is equivalent to the route print command.

Combining Netstat commands with Task Manager in Windows XP will allow you to determine active TCP/IP ports.

> 🖫 Another option you should become familiar with in addition to Netstat is the Port Reporter tool. You can find a full description of this tool on Microsoft's Web site (http://support.microsoft.com/default.aspx?scid=kb;en-us;837243).

Use Antivirus Software

Using antivirus software is a necessity. Not only must antivirus software be installed on all servers and workstations but virus definition files (DATs) must be constantly updated. If your environment is large, consider purchasing antivirus software that has a management component that allows automatic DAT updates and virus scans over the network as well as provides central administration features.

In addition to making sure that the antivirus software is up-to-date, you can block specific file types from delivering through your firewall or email system. The following list highlights the most common virus-targeted file types:

- .bas—Microsoft Visual Basic class module
- .bat—Batch file
- .cab—Cabinet Installation file
- .chm—Compiled HTML Help file
- .cmd—Microsoft Windows NT Command script
- .com—Microsoft MS-DOS program
- .cpl—Control Panel extension
- .crt—Security certificate
- .exe—Program
- .hlp—Help file
- .hta—HTML program
- .inf—Setup Information
- .ins—Internet Naming Service
- .isp—Internet Communication settings
- .js—JScript file

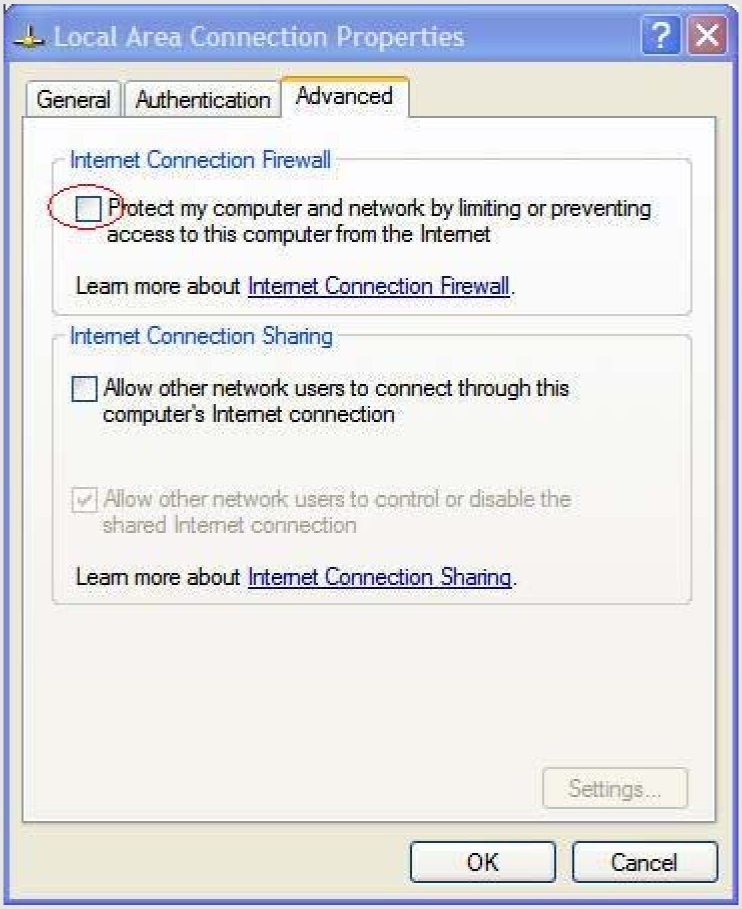
- .jse—Jscript Encoded Script file
- .lnk—Shortcut
- .mde—Microsoft Access MDE database
- .msc—Microsoft Common Console document
- .msi—Microsoft Windows Installer package
- .msp—Microsoft Windows Installer patch
- .mst—Microsoft Visual Test source files
- .pcd—Photo CD image, Microsoft Visual compiled script
- .pif—Shortcut to MS-DOS program
- .reg—Registration entries
- .scr—Screen saver
- .sct—Windows Script Component
- .shs—Shell Scrap object
- .shb—Shell Scrap object
- .url—Internet shortcut
- .vb—VBScript file
- .vbe—VBScript Encoded script file
- .vbs—VBScript file
- .wsc—Windows Script Component
- .wsf—Windows Script file
- .wsh—Windows Script Host Settings file

Use Desktop Security Software

The security features that come with OSs are sometimes not enough to meet the needs of the environment. Such is especially true with public access workstations. For that reason, desktop security software should be added when the OS cannot provide enough security.

The Internet Connection Firewall

Recent versions of Microsoft OSs include the Internet Connection Firewall (ICF), which you can enable and configure to help protect the computer from attacks. To enable (or disable) ICF on a Windows XP computer, select Start, Control Panel, Network Connections, then select the appropriate connection to the internet from the available connections (Dial-up, LAN, and so on). Select Properties, then select the Advanced tab, which Figure 1.1 shows. Simply select or clear the *Protect my computer and network by limiting or preventing access to this computer from the Internet* check box to enable or disable ICF, respectively.



Internet Connection Firewall

□ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

□ Allow other network users to connect through this computer's Internet connection

☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

Figure 1.1: The ICF dialog box.

Always Monitor Logs

Keeping a close eye on a server’s logs is one of the best ways to know when your network is under attack. Logs can show which ports are being opened, which files are being accessed, and which services are being run. Even more important, logs can show when someone has tried to log on with an incorrect password or access a resource. If your server or network is attacked, your log files are a good place to start investigating. Archive your logs on a regular basis so that the log files cannot be overwritten or erased by attackers who want to cover their tracks. If possible, configure your logs to automatically alert an IT staffer—either by sending an email or generating a pager message—if an attack is detected.

A computer running any version of Windows NT or later records events in three kinds of logs:

- Application log—The Application log contains events logged by applications or programs. For example, a database program might record a file error in the Application log. Program developers decide which events to monitor.
- Security log—The security log records events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can specify which events are recorded in the Security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the Security log. Monitoring logon attempts is a good way to detect attacks and suspicious activity. *Audit logon events* generates logon events on the local system on which the logon occurs, whereas *Audit account logon events* generates events when someone tries to authenticate with an account that is stored on the computer on which the logon event is recorded. You can configure this setting through Local Security Policy by clicking Start, Run, and typing Gpedit.msc.
- System log—The System log contains events logged by system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log. The event types logged by system components are predetermined.

Keep Software Patched

All software must be kept patched. Server and network administrators must constantly be on the alert for software vulnerabilities, and they must evaluate and install patches as soon as the patches are released. However, not all patches are necessary; administrators must first be sure that their systems need the patches. Also, some patches can cause more trouble than they are worth. If possible, test patches on a non-production system before installing them on critical servers.

Physical Vulnerabilities

It's easy to overlook physical security, especially if you work in a small or home-based business. However, physical security is an extremely important part of keeping your computers and data secure—if an experienced attacker can just walk up to your machine, it can be compromised in a matter of minutes. Although such an occurrence might seem like a remote threat, physical vulnerabilities present additional risks—such as theft, data loss, and physical damage—that make it important to check your physical security posture for holes.

When looking at providing better physical security, use the following examples to build upon:

- If at all possible, sensitive systems should be kept behind a locked door.
- A good physical security plan limits what can be done with the computers. Some examples of things you can do to stop unwanted actions is to:
  - Lock the CPU case
  - Use a cable-type security lock to keep someone from stealing the whole computer
  - Configure the BIOS not to boot from the floppy drive
  - Use the syskey utility to secure the local accounts database, local copies of Encrypting File System (EFS) encryption keys, and other valuables that you don't want attackers to have
  - Use the EFS to encrypt sensitive folders on your machine
- Keep hubs and switches behind looked doors or in locked cabinets, run cabling through walls and ceilings to make it harder to tap, and ensure that your external data connection points are kept locked.

Cost of Poor Security

The majority of vulnerabilities can be solved by patching computers, when the patches are available from the vendor. Still, even with warning after warning about potential exploits in the wild, viruses and worms continue to proliferate. Attackers continue to be successful in disrupting computing worldwide. It's arguable as to why these attacks still happen. Some blame the vendors for developing poorly written OSs and applications, while others blame the IT administrators for being complacent. Whichever side you happen to be on in the debate, there is no mistaking that security is a top issue among both sides, and that poor security not only disrupts computing but also places cost burdens on an organization.

According to the consulting firm Computer Economics, the cost of the Sasser virus to businesses worldwide is thought to be as much as $500 million. The MyDoom virus will have hit $4 billion by the end of 2004. (Although MyDoom is an old virus, it continues to spread.)

In response to the latest Sasser worm, the Gartner Group is advising its customers to budget for extra security spending on Windows desktops in the wake of all of the problems caused by the worm. Poor security results in an increase in the overall cost of owning and operating the computing environment. We will explore the costs of ineffectual or non-existent patch management throughout the rest of this guide.

> ✎ Keep in mind that if the proper patches had been applied, Sasser would not have been able to do its damage.

☞ For more information about the cost of security breaches, see the following resources:

"Survey: Costs of Computer Security Breaches Soar" at
http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/

"What Does a Computer Security Breach Really Cost?" at
http://www.securedecisions.com/documents/CostsOfBreaches-SANSInstitute.doc

SecurityDocs at http://www.securitydocs.com/

How Patching Fits into Overall Security

Granted, patching computers is only part of an overall computer security strategy, but it is arguably the most important. When you build security policies in your company, part of the policy will (or should) always include a patch management process. Although there are many ways to secure the environment and protect it from known exploits, the ultimate goal is to get the computers to the most current frame of security. This goal can only be accomplished by applying the latest security patches.

You can spend a lot of time deploying firewalls—or modifying the firewall so that open ports are closed to attack, but whenever a computer leaves the confines of the company's walls, it becomes open to attack unless it is patched against the exploit or the vulnerability is eliminated (for example, through a vendor-supplied workaround).

Security is much easier to manage when none of the company's computers leave the office desks, but employees working from home or on the road make securing the environment more complex. The reality is that more companies must support remote and mobile employees—and learn to secure an environment that includes such employees.

📖 Chapter 2 will walk through the entire patch management process and include information about how to apply patching policies to remote and mobile users.

Microsoft Patch Release Schedules

As Microsoft dominates the OS and software market, it should be no surprise that a huge importance is placed on patching Microsoft's products. Microsoft has modified its patch release schedules in the past year to better accommodate the needs of their many customers.

Monthly Calendar

Microsoft has developed the following monthly release schedule:

- Second Tuesday of each month at 10:00 A.M. Pacific Time, Microsoft Security Bulletins post, and update packages are posted on Microsoft Download Center and the appropriate update site, such as Windows Update or Office Update.
- Security alerts and bulletins are sent to people who have subscribed to the Microsoft Security Notification Service.

> ✎ Microsoft never sends notices about security updates until after the company has published information about the notices on its Web site. If you are ever in doubt about the authenticity of a Microsoft Security Bulletin notice, check TechNet to see if the bulletin is listed there (if it is not, you have reason to be suspicious).

- Press Briefings—Microsoft briefs several security industry reporters to help ensure that more customers are made aware of steps they may need to take.
- Microsoft Security Bulletin WebCast—10:00 A.M. Pacific Time, the day after release day, Microsoft hosts a WebCast and conducts a Q&A session that provides information about any "critical" or "important" bulletins. You can sign up for these and other security web casts.
- In the event of a critical vulnerability or threat, Microsoft will release a patch outside of the monthly schedule in order to better protect customers.

Security Information Resources

The following list represents some of the best resources available for learning about computer security and implementing solutions for developing secure environments.

Web Sites

Microsoft's Security Web site at http://www.microsoft.com/security is Microsoft's front page for linking to all the information about Microsoft security topics. The page shows the current security activity as well as the most current articles.

Microsoft's Security Bulletin Search at http://www.microsoft.com/technet/security/current.aspx; select the product/technology and service pack you are running to view the security bulletins that are available for your system.

Microsoft's Security Bulletin Notification Service at http://www.microsoft.com/technet/security/bulletin/notify.mspx is a free email notification service that Microsoft uses to send information to customers about the security of Microsoft products. The goal of this service is to provide customers with accurate information that they can use to inform and protect themselves from malicious attacks.

Report Microsoft Security Vulnerabilities at http://www.microsoft.com/technet/security/bulletin/alertus.aspx; the Microsoft Security Response Center investigates all reports of security vulnerabilities affecting Microsoft products. If you think you have found a security vulnerability that affects a Microsoft product, contact the company.

Microsoft's Virus Alerts at http://www.microsoft.com/technet/security/alerts/default.mspx lists current Microsoft Product Support Security Response Team virus alerts, with the most recent alerts listed at the top. For technical details, impact, prevention, and recovery information, you click the link for the virus alert you are interested in. You can call (866) PC SAFETY for free virus and security patch related support in the United States and Canada, from Microsoft.

Secunia, a leading provider of IT-security services, provides information for multi-platform security at http://www.secunia.com.

Cert.org at http://www.cert.org is a center of Internet security expertise. CERT is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Reporting Security Incidents to Government Authorities

The FBI encourages the public to report any suspected violations of United States federal law. Never think that your security incident is insignificant. Your incident might be part of a larger attack or the beginning of a larger attack. You can find your local FBI Field Division information at http://www.fbi.gov/contact/fo/fo.htm.

Security Training

Microsoft Security Training at http://www.microsoft.com/seminar/events/security.mspx

SANS Institute at http://www.sans.org/

MIS Training Institute at http://www.misti.com/

Antivirus Applications

Command AntiVirus at http://www.commandsoftware.com/ is available in useful 30-day trial versions for Windows, Linux, Netware, DOS, Exchange, and Lotus Notes

eSafe at http://www.ealaddin.com/esafe/ is antivirus software for Windows 95/98/NT/2000/XP

InVircible at http://www.invircible.com/ detects viruses, worms, Trojan Horses, hacking tools, backdoors, and so on without needing a virus-pattern database

Solo at http://www.srnmicro.com/ detects and removes viruses; the system integrity checker protects against Internet worms, backdoor programs, malicious VB and Java scripts

McAfee offers 30-day antivirus software evaluation versions at http://download.mcafee.com/eval/

NOD32 at http://www.nod32.com/products/nt.htm is available in 25-day antivirus evaluation versions; the program is smaller than 2MB in size, contains an active virus monitor, POP3 scanner, and on-demand scanner

Protector PLUS at http://www.pspl.com/ offers 30-day antivirus software evaluation versions for Windows, DOS, and NetWare

QuickHeal at http://www.quickheal.com/ offers 30-day antivirus software evaluation versions

Kaspersky at http://www.kaspersky.com/ provides useful trial versions for Linux, DOS, and Windows that offer real-time protection against Trojan Horses, backdoors, logic bombs, macro viruses, and so on

Norman at http://www.norman.com/ has antivirus and firewall trial versions for Windows, Linux, Novell, and OS/2

Norton Anti Virus at http://www.norton.com/ offers trial versions

Panda Software at http://www.pandasoftware.com/activescan/com/default.asp?language=2 provides antivirus software trial versions

Sophos at http://www.sophos.com/ offers antivirus software trial versions

Free Antivirus Applications

AnalogX at http://www.analogx.com/contents/download/system/sdefend.htm protects against script viruses (those viruses that use, for example, Visual Basic Script or Java Script) and gives a warning when scripts are executed

Antidote Super Lite version at http://www.vintage-solutions.com/English/Antivirus/Super/index.html is a freeware lite version of the commercial Antidote program; this version utilizes the same virus database as the commercial version

Anti-vir at http://www.free-av.com/ is free antivirus software for Windows that detects and removes more than 50,000 viruses; free support

Avast! at http://www.avast.com/ offers an antivirus program for Windows 9x/Me/NT/2000/XP; the home edition is free for noncommercial users

AVG Free edition at http://www.grisoft.com/us/us_index.php is a free antivirus program for Windows

BitDefender at http://www.bitdefender.com/bd/site/downloads.php?menu_id=21 provides freeware virus scanners for Linux, MS Dos, Palm, Windows CE, ICQ, and Messenger

Bootminder at http://www.freebyte.com/bootminder prevents infection from boot-viruses through floppies

Clamb av at http://www.clamav.net/ is a GPL antivirus toolkit for UNIX; the main purpose of this software is the integration with mail servers (attachment scanning); the package provides a flexible and scalable multi-threaded daemon, a command-line scanner, and a tool for automatic updating via the Internet

FProt at http://www.f-prot.com/f-prot/products/ is free antivirus software for Linux, FreeBSD, and DOS (personal use); there is an evaluation version for Windows

HandyBits at http://www.handybits.com/vsi.htm is free for personal use; after performing an auto-search for installed virus scanners, this tool will scan your files using all found installed virus scanners, which is useful functionality—some antiviral programs are good for only one type of virus

VCatch at http://www.vcatch.com/download.html is a free virus scanner for Windows that includes email protection and protection while browsing the Web

Online Virus Scanners

If you need to scan a system without loading antivirus software or you need remote workers to verify their systems' security, use an online virus scanner

BitDefender at http://www.bitdefender.com/scan/licence.php

Command on Demand at http://www.commandondemand.com/eval/index.cfm

Kaspersky at http://www.kaspersky.com/remoteviruschk.html

Panda Software at http://www.pandasoftware.com/activescan/com/activescan_principal.htm

PCPitStop at http://www.pcpitstop.com/antivirus/default.asp

RAV at http://www.ravantivirus.com/scan/

Symantec Security Check at http://security.symantec.com/

Trend Micro at http://housecall.trendmicro.com/

Spyware/Adware Detection and Removal Applications

AdAware at http://www.lavasoftusa.com/software/adaware/

Spybot Search and Destroy at http://www.safer-networking.org/

Email Discussion Lists

PatchManagement.org's list at http://www.patchmanagement.org is the industry's first discussion list dedicated to discussing security patch management topics. This list discusses the how-to's and why's of security patch management across a broad spectrum of OSs, applications, and network devices. This list is meant as an aid to network and systems administrators and security professionals who are responsible for maintaining the security posture of their hosts and applications.

myITforum's AntiVirus list at http://www.myitforum.com/articles/14/view.asp?id=1301 is an unmoderated list that promotes community discussions for antivirus products for support and review and current virus reports. The list also has a companion Web forum at http://www.myitforum.com/forums/tt.asp?appid=43.

NTBugTraq at http://www.ntbugtraq.com/ is a mailing list for the discussion of security exploits and security bugs in NT, Win2K, and Windows XP plus related applications; NTBugTraq is heavily moderated.

SecurityFocus' BugTraq at http://www.securityfocus.com/archive is a mailing list denoting security exploits and bugs covering multi-platform environments and OSs.

Microsoft Security Newsgroups

You can get help and answer the questions posed by others in the following Microsoft security newsgroups.

General Security at http://www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.security&lang=en&cr=US; News Reader version at news://msnews.microsoft.com/microsoft.public.security

Security HfNetChk at http://www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.security.hfnetchk&lang=en&cr=US; News Reader version at news://msnews.microsoft.com/microsoft.public.security.hfnetchk

Security MBSA at http://www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.security.baseline_analyzer&lang=en&cr=US; News Reader version at news://msnews.microsoft.com/microsoft.public.security.baseline_analyzer

Security Toolkit at http://www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.security.toolkit&lang=en&cr=US; News Reader version at news://msnews.microsoft.com/microsoft.public.security.toolkit

Security Virus at http://www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.security.virus&lang=en&cr=US; News Reader version at news://msnews.microsoft.com/microsoft.public.security.virus

If you're concerned with your privacy when posting to newsgroups, employ the following suggestions:

Use a modified email address—Use a different version of your email address that others will understand but that spam tools can't automatically pick up and add to their mailing lists. For example, if your actual email address is emailname@account.com, use emailname(removethis)@account.com as your modified email address.

Use a secondary email account—Set up and use an email account through providers such as Hotmail or Yahoo that is separate from your primary account. Use this account for posting to discussion groups.

Summary

As we have explored in this chapter, there is a great need for effective security in the IT market. The result of exploited administrative, product, and physical vulnerabilities can result in a company's significant loss of productivity as well as considerable monetary expense.

Although this chapter focused on overall security, it laid the groundwork for a detailed discussion of the critical security role of patch management. In the next chapter, we'll delve into patch management by exploring how to apply patching policies to remote and mobile users.