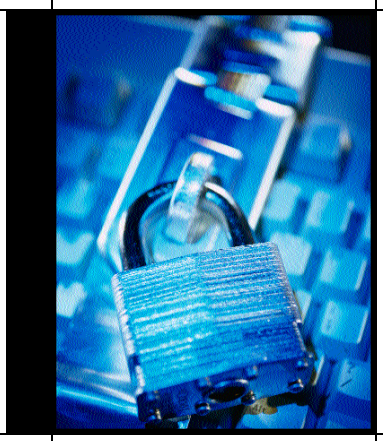
September 2000 Issue

FOCUS

YOUR SOURCE FOR INFORMATION ON COMPUTER TECHNOLOGY



Welcome to the latest issue of CDW Focus. When it comes to protecting your computer assets, you can't be too careful nor have too many ways to secure your networks and your applications. The number of e-mail viruses is on the rise and the news is filled with reports of the latest underage computer hacker to "deface" various famous sites or to clog up their traffic. Your corporation could easily become the next target.

Most attacks happen from the inside rather than the outside, however, but the principles for securing your networks and your desktops are pretty much the same. You need to understand the balance of price, features, and ease of use when it comes to implementing various security features such as virus scanners, firewalls, and encrypted e-mail. This issue of CDW Focus will offer some advice on how to protect your computer and your network from intruders and people who want to harm your data.

Setting up antivirus protection

One of the first lines of defense against intruders is to keep viruses out of your computer. Viruses can enter your machine at several points: removable media such as floppies or zip disks can become infected on one person's machine and contaminate another's when the disks are exchanged and read. Or someone can send you a virus (either intentionally or not) via an e-mail attachment. Viruses can arrive as part of a Word or PowerPoint document, hiding inside an otherwise innocuous file. Or you can download them inadvertently when you are downloading some legitimate file from the Internet.

To protect yourself, you need antivirus software. This software can be set up to automatically scan your removable media and incoming files for known viruses. The software even comes pre-loaded on many new computers, making it relatively easy to be vigilant in protecting your network.

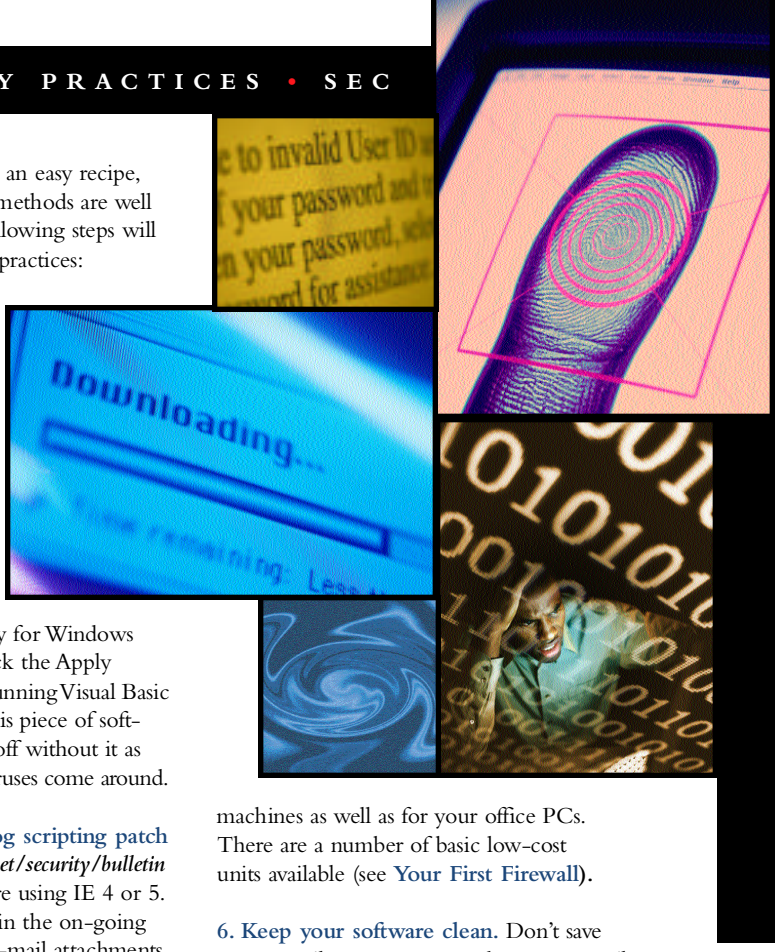
Of course, it's not quite that simple. There is an ever-escalating war between virus creators and antivirus software authors. Not long after someone creates a new virus that is able to avoid the scanning technologies present in the antivirus software, the antivirus software authors figure out the virus's "signature" and add it to their scanners. In order to maintain a high level of protection, you have to update your antivirus software regularly.

While there are many antivirus programs available, we recommend using either Symantec's Norton AntiVirus or McAfee's software. Both are created by well-established companies who are leading the pack in developing scanning and detection technologies. You can examine each company's products along with lots of good security information at their respective Web sites (see *Security Quick Clicks*). Here's how to set up Symantec's Norton AntiVirus software; the steps for McAfee are very similar.

The Norton AntiVirus software comes in several different packages: Norton AntiVirus Enterprise Solution, which includes the AntiVirus desktop software along with other software designed to protect e-mail gateways and firewalls; Norton AntiVirus 2000, for home and small office users of all Windows operating systems; and Norton AntiVirus for Macintosh. Obviously, the first step is to choose and then install your software.

Next, you need to download the latest virus signature files from Symantec's Web site. Even recently purchased antivirus software requires this step. The initial series of files is about 5 MB; subsequent updates aren't much more than a few hundred kilobytes. After you download the files, the software will ask you if it is okay to install them. With your permission it will then update your signatures to ensure that your software will recognize the most recent viruses out there.

TABLE OF CONTENTS



Note that if you plan on upgrading your system from Windows 98 or NT to Windows 2000, you'll first have to uninstall the antivirus software, then upgrade your operating system, then reinstall the software and redo the updates for the virus signatures. While this may seem like a lot more work, it is important to follow these steps precisely—if you don't, your system may become unstable.

If you need to protect multiple desktops over a network, you should consider purchasing Symantec's System Center. This is an essential tool for any enterprise: it allows you to distribute virus updates across your entire enterprise, making sure that all computers have the latest protection methods and virus signatures. It installs on an NT server and communicates with all of your desktops over your local-area network. Without this software, you would have to go around to each individual desktop and update the virus signature files manually.

Finally, you have to set up the software to scan the appropriate potential sources of infection. Removable media, e-mail, and Word documents pose the greatest risk. If you have already installed Microsoft Office, Norton AntiVirus will recognize this and set itself up to protect you automatically in these areas. This means that each time you attempt to open an e-mail attachment or a Word file, the scanning technology will take over for a brief instant and examine the file for a virus. If the file is clean, you can proceed to work with it. If it finds a virus, then it will present you with a warning to either delete the file entirely or remove the virus. You can also set up Symantec's Norton AntiVirus software to scan periodically your entire hard drive for potential infections (which you should do at least once a month) and automatically request regular updates from the Symantec Web site or System Center server.

Best practices for safe e-mailing

Employing virus-protection software isn't the only thing you should be doing. If you are concerned about receiving e-mail attachment-style viruses, such as the I Love You and BubbleBoy strains that infected corporate networks earlier this year, you might want to take some time to tighten up your security settings under Windows.

Unfortunately, there isn't an easy recipe, but these precautionary methods are well worth their time. The following steps will promote safer e-mailing practices:

1. Disable Windows Scripting Host, which is one way BubbleBoy and other scripting-style viruses get into your office. Go to Settings | Control Panel | Add/Remove Programs | Windows Setup | Accessories | Details and uncheck the box next to the entry for Windows Scripting Host. Then click the Apply button. Unless you are running Visual Basic scripts, you won't miss this piece of software and you are better off without it as more BubbleBoy-type viruses come around.

2. Download the Eyedog scripting patch ***(www.microsoft.com/technet/security/bulletin/ms99-032.asp)*** if you are using IE 4 or 5. This plugs another hole in the on-going effort to prevent rogue e-mail attachments from taking control of your system.

3. Change your Internet security options to prevent scripts from running. This is probably the best method to stop most attachment-style viruses, but you have to spend some time investigating the various options available to you. Go to Tools | Options | Security | Zone Settings | Custom | Settings under IE. Then go down the list of security items and make sure each one is set to Prompt at a minimum. You might want to choose Disable for Java, Active scripting, and Scripting of signed ActiveX controls. The exact settings depend on which browser version you are running (Outlook 2000 has a special Attachment Security button which you should set to High) and how paranoid you are (do you want to turn off cookies and scripts entirely, or just receive warnings when you receive them?).

4. Update virus signature files using the auto-update routines provided in your virus-protection software. Both Symantec's Norton AntiVirus and McAfee's software do this quite easily if your PC is connected to the Internet: all it takes is a few minutes to download the new files and update your software.

5. Consider installing a firewall or some other basic protection for your home machines as well as for your office PCs. There are a number of basic low-cost units available (see **Your First Firewall**).

6. Keep your software clean. Don't save your e-mail account password on any e-mail software. Make sure you actually delete messages after you are finished with them—software programs like Microsoft Outlook place deleted messages in a Trash folder, which you then have to explicitly empty.

7. Last, but not least: consider **not accepting any further e-mail attachments, period.** This is probably the most secure method. If you are using Outlook, you can create a rule (under Tools | Rules Wizard) to delete all messages that are sent to you with attachments, unread. This is a very drastic step, to be sure, but one that will provide a great deal of piece of mind. Otherwise, don't open unexpected attachments. Even attachments from people you normally correspond with and know might not be safe.

Best practices for secure applications integration

In addition to protecting your e-mail, you should spend some time with your other applications as well. Here are a few suggestions from Peter Coffee of eWeek and others:

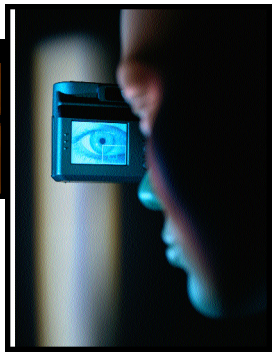
— Educate users on the potential harm of e-mail attachments, active-content Web sites, and downloaded code.

— Consider using something other than Word to read e-mail attachments, such as WordPad, or share documents in Revisable Text Format or straight text, which can't be infected with macro viruses.

— Document costs of end-user productivity loss and IT staff distraction to justify budgets for security training and tools.

— Acquaint user support personnel with application options and their potential security effects, documenting recommended settings.

— Investigate sources of information on security vulnerabilities of locally used applications, including both free updates (such as vendor Web sites) and extra-cost alternatives (such as premium support plans or third-party consultants).



Your first firewall

Most people, when they think about protecting their network from attackers, think about firewalls. Firewalls offer the best and most basic form of isolating internal network users from the big, bad outside world of the Internet, as well as just plain curiosity seekers. But firewalls come in all shapes, sizes, and prices.

A firewall is simply a machine with at least two network connections, typically one to the outside world and one to your internal network. It provides a modifiable list of rules that allows you to block the things you don't want (such as packets, applications, or kinds of connections) and allow the things you do. The trick is in how you set up these rules.

Most large corporate networks have firewalls protecting their enterprises that cost tens of thousands of dollars. But if you have a continuous Internet connection at home, or if you have a series of remote branch offices, these devices are overkill. You can buy some peace of mind for less than $1,000 if all you need to protect is a typical small or home office. CDW sells three of these units, the WatchGuard SOHO, the SonicWALL SOHO, and the 3Com OfficeConnect. Each of these units is very easy to set up and maintain.

All of the units are configured with a Web browser—once you set up your IP network properly, you can do all of the remaining set up using a series of graphical screens that are, for the most part, fairly obvious. Each unit differs in terms of its default protection settings and the flexibility of its features. All support Network Address Translation (see Setting Up NAT), a way to further discourage prying eyes and keyboards from entering your networks.

The WatchGuard is perhaps the simplest of these three. It comes with a dynamic host configuration protocol (DHCP) server, so you don't have to worry about setting IP addresses for your home network. It also detects a DHCP server at your ISP or cable provider, so you don't have to worry about configuring it for the wide-area link either. And all of its documentation amounts to a single page. Also appealing about the WatchGuard is that the unit's default settings offer a solid level of network protection.

But the WatchGuard is fairly basic. You can't do much with it. If you need more, then consider the SonicWALL or the 3Com OfficeConnect (essentially the same unit), a step up from the WatchGuard in terms of complexity, features, and price. Both the Sonic and 3Com firewalls have a great system for setting up firewall rules and filters to block or allow various kinds of protocols, ports, applications, and other details. These units are useful if you want to grant access to a particular computer inside your firewall, say a Web server on your home network that you want to have access to from your office. You'll have to know a few things, such as the fact that Web applications operate on port 80 and FTP on port 21, to set up these rules properly. Unfortunately, the Sonic and 3Com manuals don't do the best job of explaining how to do this.

The SonicWALL and WatchGuard are available for 10-user networks. The 3Com unit handles 25 users, and Sonic sells a 50-user license as well.

Firewalls are good protection and make sense even for the average citizen. The units described here offer basic protection without the hassle or expense of hiring professional security consultants.

CDW Part Numbers

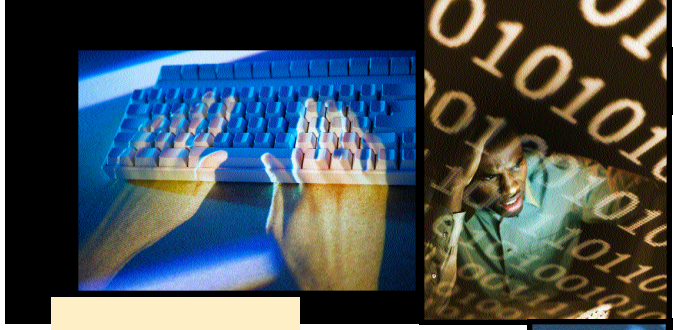
WatchGuard SOHO/10 users	203126
SonicWALL SOHO/10 users	190876
SonicWALL SOHO/50 users	190877
3Com OfficeConnect Internet Firewall/25 users	199852

Setting Up NAT

One of the easiest things you can do to protect your network from hackers is to set up Network Address Translation or NAT. NAT is useful for hiding the "real" IP address that each machine on your network actually uses by providing a fake address that works only inside your local-area network or firewall. Typically, a network administrator maps a series of inside IP addresses to one IP address that is used on the outside of its firewall. Each incoming IP packet must go through this translation process, and various authentication mechanisms can be used to determine if the incoming packets are legitimate requests (such as responses from Web servers for requests to view particular pages) or not (such as denial-of-service and other attacks).

NAT also has the side benefit of conserving actual IP addresses, in case your corporation is running out of address space and chooses not to, or can't, obtain additional IP addresses from your Internet provider. It lets your company use a single IP address in its communication with the outside world.

While it isn't the only thing you should do, NAT can accomplish several things at once for little or no extra cost—most routers and firewalls, including the SOHO firewalls mentioned earlier, come with support for NAT built-in, and cost only the time it takes to configure it. This is easily done on the SonicWALL program by selecting DHCP with NAT enabled on the General | Network configuration page and then rebooting the router. With other routers, you might have to use a series of command lines to enable NAT. (With Cisco routers, it is a simple "set nat enabled" then "write" to store the changes, and rebooting the router.)



Using Shields UP! to probe your network defenses

Setting up NAT and firewalls is fine, but you'd also like to test your network from time to time to make sure no loopholes exist. There are several products that can help here, and one in particular should be on everyone's short list: Steve Gibson's Shields UP!.

Until recently, test tools to help you strengthen your defenses were both costly and complex to use. If you are a typical Windows user, you probably turn on file sharing because you want to share files with your colleagues. That's what peer-to-peer networking is all about, after all. However, this ease-of-use boon has been a cross to bear for IT administrators. Without your knowledge, you may be making these shared files available over the Internet. Clearly this is a problem, particularly if you need to share files locally but don't want everyone in the world to see them too. What to do? Go to Gibson's Web site (www.grc.com) and run this test tool.

Shields UP! is a very effective and simple tool. It answers the question: What am I vulnerable to attack from over the Internet? Besides shared files, there are well-known TCP/IP communication ports that are usually prone to probing and attack from the outside. These ports, such as 80 for Web servers, 23 for Telnet sessions, and 21 for FTP sessions, can be closed off with the appropriate Windows commands. Shields UP! not only tells you if someone has left a back door to your system unlocked, but it also tells you what to do about it—you get practical information on how to secure your system and keep your assets protected.

Gibson has provided lots of advice on how to correct the problems Shields UP! discovers. This advice is actually more important than doing the tests themselves because it will get you thinking about how your system is exposed and how hackers think as they look for ways to force entry.

If you have a continuous Internet connection you should run Shields UP!—and run it on all Internet-connected computers in your enterprise. It takes a few minutes to do a test that can save you hours of headaches down the road. In addition to running this tool, you might want to consider protecting your computers by properly setting up Windows file sharing.

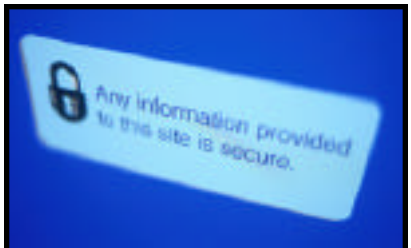
How to set up Windows file sharing securely

One of the biggest security weaknesses with any desktop is its ability to become an instant file server, allowing you to share files with the world at large. While this is certainly convenient (to turn this feature on, merely go to Settings | Control Panel | Network | File and Printer Sharing and click on each button to turn on the ability to share both your files and your local printers with the world. You'll also have to open up Windows Explorer, right-click on the directory you'd like to share, and enable sharing.

Doing this has wide implications: your PC is now sending out a special "broadcast" message every minute or so, telling everyone on your network (and if you have an Internet connection, by extension, on the Internet), the name of your shared resources. Within a few minutes, someone with a packet sniffer could easily find this information out.

First of all, you can better protect your shared network resources by tightening up your access security. Windows-networked shared resources can be protected in two different ways: either by specifying a share name and password for each shared resource (called share-level security) or by specifying a user name and password for each user of the shared resource (called user-level security). Obviously, the latter is more stringent than the former, and should be used at all times if possible. User-level security works best with a centralized NT or Windows 2000 directory server. To make the change on your desktop, go to Settings | Control Panel | Network | Access Control and check the appropriate box.

The trouble comes when you don't want everyone to share your files, especially everyone on the Internet. There are several ways to prevent this from happening. First, if you make use of the SOHO firewalls mentioned earlier, all of them have explicit features to block the network broadcasts from going beyond your local network to the Internet. On the WatchGuard, you have to check a special box on one of its configuration menus; on the SonicWALL and 3Com these broadcasts are blocked by default.



"You need to test your network periodically for security loopholes."

You can also set up your Windows machine to not send any Windows networking information out over TCP/IP protocols. There are two steps to this process. For Windows 98, go to Settings | Control Panel | Network | Configuration | TCP/IP Protocol for your particular Ethernet or Token Ring networking card. Then go to the tab marked NetBIOS and uncheck the box that sends NetBIOS broadcasts over TCP/IP. Also, go to the tab marked Bindings and uncheck all the boxes there, including Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks, and Microsoft Family Logon.

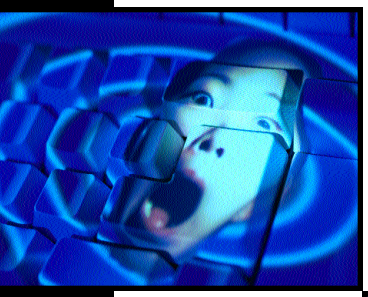
For Windows 2000, go to Settings | Networking and Dial-up Connections | Local Area Connections and right-click on Properties. Then go to TCP/IP | Advanced | WINS and check the button next to Disable NetBIOS over TCP/IP.

For either version of Windows, you have to also perform the second step, which is to remove the default file sharing that gets installed with every Windows installation. (If you don't have your machine set up to share files, then you can safely skip this step.) Go to the root of your C: drive and right-click on Sharing. Remove the default C$ share. Also go to C:\Windows and right-click on Sharing and remove the default ADMIN$ share.

Either way, you will ensure that when you are sharing your files over your local network, you are not sharing them over the Internet. More detailed instructions can be found at www.grc.com/su-rebinding9x.htm and in Security Quick Clicks (see Securing Windows 2000).

You can never be too paranoid

Fred Avolio makes his living being paranoid—after all, he is a security consultant. One of his favorite warnings concerns how people obtain their e-mail when they are traveling, especially at computer industry conferences. Here's why.



Most conferences now provide public-access computers so that attendees can check their e-mail and get work done during the show. But few people understand the implications of using these public PCs, or the importance of deleting any traces of their electronic correspondence before they walk away from the keyboard. This is a problem: the truth is that public PCs are one of the worst places to read e-mail.

For starters, data could be captured intentionally (or not) by someone demonstrating a packet sniffing device elsewhere on the show floor. Someone might be trolling for passwords just as you log on to get your e-mail. The only way to avoid this is to encrypt your session by using a virtual private network, which isn't usually available on public PCs.

And you aren't even safe in your hotel room: "At the last hotel I stayed in, each room had its own Ethernet jack. Who knew what lurker was capturing what data over that network?" says Avolio. Even at less equipped hotels, someone could be bribed to tap into your dial-up connection. The likelihood of this happening is directly related to the business you are in and how much the information is worth to, say, a corporate spy.

"Many people use Web-based mail services, such as MailandNews.com," says Avolio. "If you do, note that at the bottom of the home page there is a link to establish a secure session in which to read your e-mail. You should always use this option and get the extra protection, even though it still doesn't protect your password. To do that, try e-mail programs such as Eudora, which provide a mechanism called APOP to protect against sending unencrypted passwords. Unfortunately, few ISPs support this mechanism."

Speaking of passwords, you should change them today and then again before you head out on the road to your next conference. If your e-mail password is the same as your dial-in or log-on password, you are running a big risk. Use different passwords for each, and choose ones you can memorize, so you don't have to write them down.

Of course, your company should have an information security policy that includes a description of the circumstances in which employees can use public PCs for company business.

Another problem is the public PC's configuration. You can't tell if you are using a real copy of IE or Netscape or a facsimile holding a Trojan horse that is ready to capture your password information or data. Granted, this is an unlikely scenario, but it has happened.

Even if the public PC you are using is pristine, you still have to clean up after yourself. For example, if you change the personal information in the browser (e.g., name, e-mail address, POP mail account, password), remember to delete all of this before you leave the PC. If you forget, the next person can download e-mail from your account, or send messages masquerading as you.

Similarly, if you downloaded and read any e-mail, be sure to delete it all before leaving the PC. Otherwise, anyone stopping by will be able to read your correspondence. Lastly, don't forget to clean out the In, Out, Sent, and Trash mailboxes. Some software programs will prompt you to delete the messages in each mailbox and empty the trash before exiting the program. Some don't. "I have seen many PCs containing mail from the previous user. It happens more often than you think," says Avolio.

Finally, if you are using the more recent vintage of either browser, before you type in personal information make sure that they are not set to store passwords or to fill in forms automatically. These browsers can recall this information for the next user.

It is amazing how many people forget these last steps. So be a little paranoid—protect your e-mail correspondence.

Encrypting your e-mail

These are all good suggestions if you want to be a little bit paranoid about your e-mail habits. However, some people feel that their correspondence just doesn't present much of a target. They aren't famous, their businesses aren't well known, or they don't handle very sensitive documents. Yet what they don't realize is that just about anyone can read any e-mails sent over the Internet. If you have the time, the tools, and the technical know-how, you can capture this traffic. Then (if you also have the malicious intent) you can impersonate someone's identity and do a great deal of damage. For example, you could send subscription requests to a variety of e-mail newsletters and bury someone's mailbox in unwanted messages. Or you could assume someone's electronic identity and send sensitive information to the wrong party.

The issue is that all messages sent over the Internet are in clear text, unless otherwise protected. If this text is intercepted, its contents can be viewed, altered, or otherwise interfered with. While this scenario may be unlikely, it's important to realize that it can be accomplished if someone is determined enough to do so.

Given the risks, the best solution is to employ software to encrypt your e-mail. So why don't more people do this? Because encryption is difficult to set up, has poor interoperability with other correspondents, and is, in general, plagued with problems. You'll have to deal with choosing the right technologies, maintaining your keys and passphrases, and actually performing the necessary operations to encrypt and decrypt your messages.

The problem is that you and all of your correspondents need to implement the same encryption scheme in order for all of the cloak-and-dagger stuff to work. You

Quick Clicks

Antivirus Research Centers
McAfee: www.mcafeeb2b.com/asp_set/anti_virus/avert/intro.asp
Norton: www.symantec.com/avcenter/index.html
Two of the best places to learn about how to ward off viruses and attacks on your computers as well as where to go to download the antivirus software you need to defend yourself. Both companies also post up-to-date information on the latest viruses to make their rounds on the Internet.

Microsoft Security Patches
www.microsoft.com/security
Lots of patches, fixes, and suggestions on making your Windows operating systems more secure. Also includes a good tutorial series on security basics.

SecurityFocus.com
www.securityfocus.com
Here's a comprehensive security-information Web site—complete with patches, suggestions, and links to numerous products. Information is categorized by operating system and application, and the site contains a full list of Microsoft Windows security patches and warnings. You'll also find other useful tools and articles on general security procedures and policies.

AINTX, an NT Administrative Toolset
maxx.mc.net/~jlh/nttools/html/nttools.htm
A series of command-line utilities that enable someone with previous Unix knowledge to manage similar tasks on NT, such as deleting printer jobs, changing users passwords, and editing access control lists.

Securing Windows 2000
www.arstechnica.com/tweak/win2k/security/begin-1.html
Jeremy Page of Ars Technica presents a detailed but solid step-by-step prescription for locking down your Windows 2000 machine.

Entrust's Security Resources
www.entrust.com/resourcecenter/references.htm
The place to locate books, links, and other helpful resources for information on general security topics.

Defaced Web Pages Archive
www.hackernews.com/defaced/1999
A collection of Web pages that have been altered by hackers, along with links to their current (and hopefully pristine) locations. The list of targets ranges from private corporations to government sites.

Hacking Exploits
advice.networkice.com/advice/exploits
A technical description from Network ICE of various hacking techniques and ways to prevent them.

can't just decide to encrypt your e-mail without getting others involved, unless you don't want anyone else to read your correspondence. (Perhaps this is the ultimate in e-mail security, but it isn't a very useful one!)

There are two major technologies used today for e-mail encryption: one, called Pretty Good Privacy (PGP), began with a private developer and is now owned wholly by Network Associates. The other one is loosely based on emerging standards and is called Secure/MIME (S/MIME). PGP is everyman's product. It was designed for single individuals to use and still remains the easiest method to set up and deploy, although it is far from simple. It comes inside the box of Eudora Pro but isn't very well integrated into the program.

While PGP is a single-vendor solution, numerous vendors offer S/MIME, although in practice you will probably want to limit yourself to a single vendor to avoid interoperability problems. Not all S/MIME packages can exchange encrypted e-mail with each other, owing to differences in their implementations. Both Netscape Messenger and Microsoft Outlook Express include support for S/MIME. See the table below for a more complete list of products and Web locations from which to download the various programs.

Where to start? We recommend using Netscape's software if you intend on receiving encrypted messages from multiple e-mail clients and correspondents. It is able to decrypt the most messages coming from others. If you intend to be on the other side of the fence, we recommend Outlook Express: it appears to be the best "donor" for sending encrypted messages to others.

An alternative to these commercial packages is to use one of a number of free products that provide encryption services. Companies such as PrivacyX.com, Zero-Knowledge, and others have begun to offer ways to use encryption without all of the hassles of their commercial competitors. While these products aren't as easy as using plain-text e-mail products, they do offer ways to provide extra security without too much extra effort or cost.

Name, Vendor	URL
PGPmail, Network Associates	www.pgp.com
ArmorMail, LJL Enterprises	www.ljl.com
Messaging Management System, Tumbleweed Communications	www.tumbleweed.com/worldtalk.html
InvisiMail, InvisiMail International Ltd.	www.invisimail.com
Outlook Express, Microsoft	www.microsoft.com/windows/ie
Messenger, Netscape	www.netscape.com
MailSecure, BaltimoreTechnologies	www.baltimore.com
ExpressMail, OpenSoft	www.opensoft.com

Securing your e-commerce server

Your Web storefront is the front door for potential attacks on your corporate data, and it makes sense to put your strongest security measures in place here. But, as Anup Ghosh suggests in his book, E-Commerce Security, it will take more than just adding a few locks.

— *Set access control appropriately for all server software files, limiting access to intended administrators. Users outside the Web operations team should not have read/write permissions to any files in the server root.*

— *Configure servers to switch executing privileges to a non-privileged user wherever possible.*

— *Turn off automatic directory listings and disable server side includes and symbolic linking.*

— *Restrict access to sensitive Web pages based on a client's IP address or host name.*

— *Keep current with software updates to your server software, and be on the lookout for patches that effect security changes.*

— *If possible, use digital certificates to ensure secure access.*

— *Test and test again any scripts used in your storefront for security vulnerabilities. Limit the directories where these scripts reside and configure them properly.*

How One Enterprise Handles Security

So far we have discussed many ways to improve the security of your network with various tools and techniques. So what kind of security does a typical enterprise actually put into place? In one case, it turns out they do a great deal of what we have recommended.

Sam Blumenstyk is the Manager of Network Engineering for White & Case LLP, an international law firm supporting over 2,500 people in 35 cities, from Bahrain to Paris. The company maintains 10 Web servers, 100 file servers, and 15 Cisco routers.

The first line of White & Case's defense is a Check Point Firewall-1 that is maintained by internal staff with assistance from outside consultants. The staff is constantly modifying the configuration to meet the diverse needs of the firm, including creating new filtering rules, opening up well-known ports to specific applications and specific IP addresses, testing problems, and diagnosing error logs. The Check Point implements Network Address Translation to ensure that no internal IP address is ever exposed to the outside world.

Behind the Check Point firewall is a "demilitarized zone" of specialized servers. This zone is visible to both those on the outside Internet as well as those on the internal network, and includes e-mail, FTP, and one of their Web servers. "We set up our production servers to have some limited trusts of the servers in this zone. This way, users attach to servers in the zone and not to the production network," says Blumenstyk.

Most of the firm's Web hosting is done with an external provider. While this was not initially done for security reasons, Blumenstyk admits that it helps in this department.

The firm also has implemented the virtual private network feature of Novell's BorderManager. Initially, they have used this to secure communications from server to server across their international wide-area network, but they are exploring using it with VPN clients as well. Eventually, the firm plans on migrating to NetWare 5 and implementing directory services for enterprise-wide authentication as well. In addition, the firm has outsourced its remote connections with Infonet's Remote Authentication Services network. Anyone who needs remote access to White & Case's wide-area network dials up to Infonet's network and provides the appropriate authentication. They then enter the firm's wide-area network through a series of rules at the firewall. "I don't have to worry about resetting modems all day long—and Infonet works with the existing authentication schemes on my network," says Blumenstyk.

The firm has a wide variety of e-mail security systems (which is not surprising, given the nature of communications between attorneys and their clients). They have about 20 users of PGP at the requests of various clients. Other clients have direct connections between their e-mail systems and White & Case's, typically with gateways and modems or using private network connections that bypass the Internet.

Finally, the firm has a group of software administrators who work as part of the help desk team. These staffers are responsible for adding and removing users, and they have a written protocol to follow when someone leaves the firm. "Our Help Desk is very responsive in handling people that leave the company," says Blumenstyk.

Hackers Dictionary

To understand how to defend yourself against network attacks and intruders, you have to first understand the lingo. Here is a brief lexicon on various vulnerabilities:

Back door—a hole placed in the security of a system deliberately by designers or programmers. Usually, a back door is created for ease of maintenance of a particular system. However, it can become a security issue, particularly if the designer is fired or departs under other unfortunate circumstances.

Boot sector virus—a nasty virus that is usually found on floppies. When a user launches one, it infects the boot sector of the hard drive and runs when the computer is restarted.

Denial-of-service (DoS)—an attack whose purpose isn't to break into a system, but simply to deny anybody else from using it. DoS attacks come in many different forms, but all result in a blocked server.

Mail bomb—massive amounts of e-mail sent to a single destination, in the hopes of overwhelming a particular server and disrupting service.

Macro virus—a particularly insidious virus that contaminates Word and other Microsoft Office documents. When a user opens the document, the virus is launched.

Password grabber—a program, usually hidden, which copies legitimate passwords into a special file to provide hackers the information they need to gain entry into a system.

Spoof—to capture, alter, and retransmit a series of packets in a way that misleads the recipient. This usually refers to altering

Session hijacking—when a hacker takes over a TCP session between two machines. This enables the hacker to gain access to a machine as a legitimate user.

Syn flood—an attack that sends TCP connection requests faster than a machine can process them, typically resulting in a crashed server.

Trojan horse—a computer program that disguises itself or its true malicious purpose inside another more benign program. The Happy99 program is one example: when recipients clicked on this e-mail attachment, the program launched a brief display of fireworks. While the user watched, the program modified the user's e-mail program to allow it to send itself out in subsequent messages to others.

Worm—a program that exists to propagate itself, sending copies via various means, such as e-mail or Internet Relay Chat. A worm can infect a computer's memory or hard disk and then send copies of itself to other computers.

Making Your Enterprise More Secure!

- Setting up your first firewall
- Encrypting your e-mail
- Securing your e-commerce server
- Tools to probe your network security
- Rules for receiving virus-free e-mails

CDW Computer Centers, Inc.
200 N. Milwaukee Avenue
Vernon Hills, IL 60061