

ITPro<sup>TM</sup>  
SERIES

WindowsITPro

 **eBooks**

Keeping Your Business  
SAFE from Attack:

# Monitoring and Managing Your Network Security

By Douglas Toombs

**Microsoft<sup>®</sup>**



## Contents

<b>Chapter 1 Securing Your Network</b> .....	<b>1</b>
<b>Trustworthy Computing—What Has Happened and What’s to Come</b> .....	<b>2</b>
The Evidence of Patch Releases .....	3
<b>Security Initiatives in Trustworthy Computing</b> .....	<b>4</b>
Secure by Default and Secure in Deployment .....	4
Secure by Default .....	4
Secure in Deployment .....	5
MBSA .....	5
<b>The First Step to Security: Understanding</b> .....	<b>7</b>
Threats from Outside .....	7
Defense in Depth .....	7
Additional Defenses Against Attack Techniques .....	8
Footprinting .....	8
Scanning .....	9
Enumeration .....	9
Penetration .....	9
Escalation .....	9
Getting Local .....	10
Expanding Influence .....	10
Cleanup .....	10
Threats from Inside .....	10
A Case in Point .....	10
<b>A Secure Windows Network</b> .....	<b>11</b>
<b>A Secure Microsoft Network</b> .....	<b>11</b>
<b>Next: Hardening Your Network</b> .....	<b>11</b>

## Chapter 1:

# Securing Your Network

Whether a company has networked or standalone computing, security is always a concern for IT. No one can deny that some people in the world will attempt to harm the systems and data that you oversee. Whether or not attackers know your company personally (some attacks can come from inside), the simple truth is that you must guard and protect your data with the same vigilance you would use to protect your cash assets. That might sound like an exaggeration, but it's absolutely true. And just as you wouldn't leave your operating cash lying around your office where anyone could take it, you don't want access to your data or systems available to anyone but those whom you've authorized. The potential costs of disclosing confidential data, theft, embezzlement, or extended unplanned downtime are significant. This book, *Keeping Your Business Safe from Attack: Monitoring and Managing Your Network Security*, can help you protect your company's assets.

A few recent court cases demonstrate how severe the consequences of security vulnerabilities can be. For example, one Romanian intruder and five American co-conspirators were recently indicted on charges that they conspired to steal more than \$10 million in computer equipment from Ingram Micro in Santa Ana, California. The company, which has a sales volume of more than \$20 billion per year, is the largest technology distributor in the world. The 24-year-old Romanian man ordered equipment to be shipped to his country. When Ingram Micro stopped all shipments to Romania, the intruder simply enlisted co-conspirators (all of them 20 to 27 years old) through Internet chat rooms to accept shipments in the United States. The co-conspirators then either shipped the equipment to Romania or sold it for cash. The thefts went on for quite some time, demonstrating that intruders are happy enough to steal a few thousand dollars at a time to stay under the radar and avoid being detected. Unfortunately, through Internet chat rooms, intruders can easily find co-conspirators to help execute their schemes.

Although the Ingram Micro case is a high-profile one, this type of activity takes place on a smaller scale as well. Take the case of the Vallejo, California, woman who recently plead guilty to charges that she embezzled nearly a million dollars from North Bay Health Care Group, a nonprofit healthcare organization that operates hospitals and clinics in California. The woman perpetrated the alleged crime by gaining unauthorized access to North Bay's accounting software. She then issued more than 120 checks payable to her and to others, leading to organizational losses of at least \$875,000. Although North Bay's annual revenue figures aren't public record, one can imagine that such embezzlement could put the company's financial health at serious risk. To conceal the fraud, the woman altered the electronic check register to make it appear that the checks had been paid to North Bay's usual vendors. She was apparently issuing many small checks for \$5,000 to \$10,000.

Even if people with malicious intentions aren't trying to steal money from you directly and don't know your organization personally, they can still affect your organization in terms of unplanned downtime. They can disable the critical systems that let your business function properly. Malicious hackers have caused such problems for nearly two decades —starting with the Morris worm in 1988 that crippled VAX and Sun Microsystems computers across the Internet. Although some of you might

## 2 Keeping Your Business Safe from Attack: Monitoring and Managing Your Network Security

not remember the Morris worm, you'll find the outlines of the story familiar. (I thank Charles Schmidt and Tom Darby for their Morris worm research. You can read more about the Morris worm at <http://www.snowplow.org/tom/worm/worm.html>.) The following sequence details the worm's activities.

- 6:00 P.M. At about this time, malicious hackers launch the worm.
- 8:49 P.M. The worm infects a VAX 8600 at the University of Utah.
- 9:09 P.M. The worm initiates the first of its attacks to infect other computers from the infected VAX.
- 9:21 P.M. The load average on the system reaches 5. (Load average is a measure of how hard the computer system is working. At 9:30 P.M., the usual load average of the VAX was 1. Any load average higher than 5 causes delays in data processing.)
- 9:41 P.M. The load average reaches 7.
- 10:01 P.M. The load average reaches 16.
- 10:06 P.M. At this point, so many worms are infecting the system that no new processes can start. No one can use the system.
- 10:20 P.M. The system administrator kills off the worms.
- 10:41 P.M. The system is reinfected and the load average reaches 27.
- 10:49 P.M. The system administrator shuts down the system. The system is subsequently restarted.
- 11:21 P.M. Reinfection causes the load average to reach 37.

In fewer than 90 minutes from the time of infection, the worm rendered the University of Utah system completely unusable. More than 6000 machines across the Internet experienced the same fate. Although the worm caused no physical damage, the US General Accounting Office (GAO) estimated the costs at between \$100,000 and \$10,000,000 because of lost Internet access at infected hosts.

So what should administrators do? Simply put, the answer lies in gaining the right knowledge. The single best security countermeasure for any network is a competent security professional. The problem, however, is that so many IT professionals are overworked. Author Tom Iwanski put it well in an article in *Windows & .NET Magazine*: "Human errors are inevitable, especially when administrators wear several hats."

Fortunately, by reading this book, you're doing exactly the right thing—gaining more knowledge about information security. In the pages that follow, I'll show you that security doesn't need to be a complex, fear-inducing mountain of information. Instead, you can make security an outlook, an approach, a method, and a practice—and thereby stay constantly attentive to your organization's security. Microsoft has made this task easier through a companywide undertaking begun in January 2002, known as Trustworthy Computing.

### **Trustworthy Computing—What Has Happened and What's to Come**

At the beginning of 2002, Microsoft Chairman and Chief Software Architect Bill Gates launched a new initiative within Microsoft known as Trustworthy Computing. In an internal email message to all Microsoft employees and subsequently at trade shows around the world, he drove home a number of points about what he saw as a necessity for the future of Microsoft products. In my opinion, the key component of his email message was that through Trustworthy Computing "customers will always be able to rely on [Microsoft] systems to be available and to secure their information."

The Trustworthy Computing framework comprises goals, means, and execution. The goals are the high-level objectives that Microsoft is working to achieve in the four main areas of security,

privacy, reliability, and integrity. In the following text, I discuss Microsoft's means and consider the company's execution in the area of security.

At the launch of the initiative, Microsoft abruptly halted the development work of more than 8500 engineers to perform an intensive security analysis of the Windows operating source code. In addition to the intensive audit of the Windows source code, Microsoft gave developers and engineers special training in writing secure software. The initiative cost Microsoft nearly \$100 million within the first 2 months, and trustworthy computing continues to be a guiding principle in the development process. Most importantly, the results of Microsoft's execution of the initiative are evident.

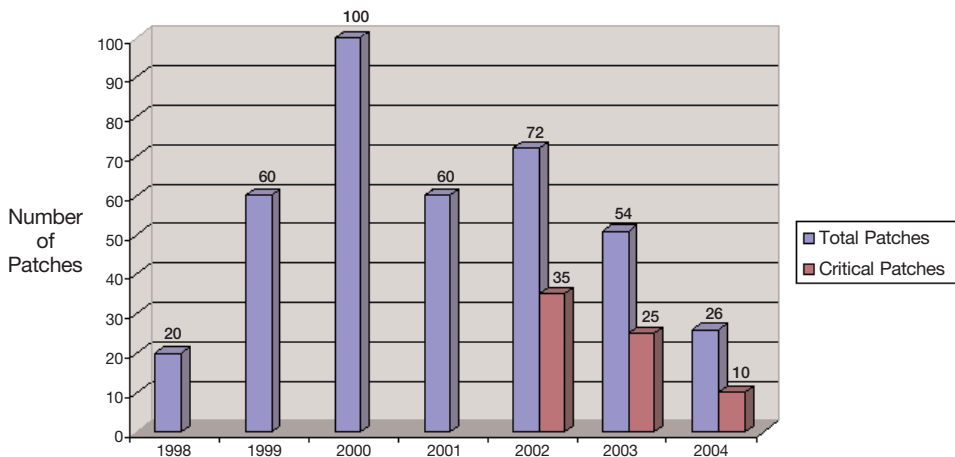
When Microsoft first started publicly discussing the Trustworthy Computing initiative, mainstream media professionals were skeptical. However, nearly 3 years later, the results are irrefutable—the initiative has had a significant impact on the security and availability of network infrastructures around the world.

### ***The Evidence of Patch Releases***

For example, the number of patches Microsoft has released has dropped each year—from 72 in 2002, to 51 in 2003, to just 26 (to date) in 2004. If you consider only those updates that Microsoft rated as “critical,” you see a similar pattern of decline—to just 10 patches released in 2004 (to date). Figure 1-1 presents the patch-release pattern over the past 7 years.

**Figure 1-1**

*Microsoft patches released from 1998 through 2004 (to date)*



Note: Because patch classification began in November 2001, no data segregating critical patches exists before that date.

Although general perception of the initiative's effects might vary, the numbers show clearly that Microsoft has improved its development process and is now releasing code that's much more secure and trustworthy out-of-the-box.

A similarly positive pattern emerges from the declining patch numbers for the first year following recent Microsoft OS releases. For example, if you compare the number of patches in the first year

## 4 Keeping Your Business Safe from Attack: Monitoring and Managing Your Network Security

after the release of Windows 2000 Server Standard Edition to the number of patches in the first year after the release of Windows Server 2003 Standard Edition, the decrease is clear. For Win2K, Microsoft released 53 patches within the first year (measured from “release to manufacturing,” the date on which the code for a Windows OS stops changing and starts getting burned onto CD-ROMs). For Windows 2003, Microsoft released just 19 patches. You can see that the need to patch the OS is becoming less common. If you take into account that 14 of the 19 patches for Windows 2003 also applied to Win2K and Windows NT (i.e., they addressed old bugs), the numbers tell an even better story about the increasing security of Microsoft OSs.

The patch figures for the first year following the release of new desktop systems follow the same pattern: Win2K Professional and Windows XP Professional had 48 and 22 patches, respectively. And of the 22 patches released in XP’s first year, 11 also applied to Win2K.

Critics who’ve lambasted Microsoft in the past about the number of patches the company’s code required have fallen quiet on this subject. Microsoft is achieving the Trustworthy Computing initiative’s first goal: security.

### Security Initiatives in Trustworthy Computing

The previous discussion points out one of the critical means for achieving the security goal of Trustworthy Computing: Code must be *secure by design*. Through steps such as the exhaustive Windows code audit I mentioned previously and improved education and development processes, the software Microsoft delivers is increasingly secure. However, Microsoft hasn’t left matters there. The company recognizes that its responsibility doesn’t end when it releases a CD-ROM to manufacturing.

### *Secure by Default and Secure in Deployment*

Microsoft realizes that a system must be secure when installed and—over its life cycle—*remain* secure by being easily repaired or patched as needed. This approach encompasses two additional means to reach the security goal of Trustworthy Computing—making systems *secure by default* and *secure in deployment*.

#### Secure by Default

For OS or application installations to be *secure by default*, the products should have built-in security measures, and all potentially vulnerable components should be disabled by default. Principles such as these are echoed by information security professionals around the world, among them SecurityFocus.com columnist Jason Miller. In his May 2004 column about all operating platforms, Miller noted, “Vulnerabilities in network-aware services [exist] ... what do we do about it? Shut them off by default.”

Microsoft is delivering on this concept with the OSs released since the launch of Trustworthy Computing—namely Windows 2003—and with legacy OSs as well. In Windows 2003, the default installation is much more secure than any previous Windows installation. A number of network-aware components enabled by default in previous Windows generations are now disabled, and default security settings are much tighter across the board. Also, new capabilities slated to be released in the first service pack for Windows 2003 will bring administrators even more security capabilities.

In addition to the improvements on the server side, Microsoft is attending to the desktop. At the time of this writing, Microsoft has just released XP Service Pack 2 (SP2)—which includes significant security improvements. By default, a computer with XP SP2 installed won’t listen for any incoming

requests from outside its own network because Microsoft now enables the built-in firewall by default. With XP SP2's default configuration, you could literally plug an XP desktop directly into the Internet (as many home users do with their broadband connections) and not worry about the system being compromised. I'm impressed with the feature set that XP SP2 provides by default, and I believe that this service pack will significantly affect network security as it makes its way to corporate desktops and home users.

## Secure in Deployment

The final step toward the security goal is to release products that are *secure in deployment*. The phrase is Microsoft's descriptive term for systems that you can easily audit and patch as needed, which will help organizations assess and manage security risks across their networks.

## MBSA

If you're concerned about your organization's security, download and deploy the Microsoft Baseline Security Analyzer (MBSA) to get the information you need to update and protect your environment. MBSA reveals which hosts need to be patched—and with which patches. With that information, you can use free applications such as the Automatic Update client and server-side packages such as Software Update Services (SUS) to perform the updating.

With a properly configured SUS installation within an organization, administrators can select updates to be deployed throughout their network. Administrators can also define all of their Windows hosts to automatically grab approved updates, install them, and even reboot themselves after installation (if required). This set of capabilities is one of the most important security improvements Microsoft has released—yet many administrators are still unaware of what it can do and how much time it can save.

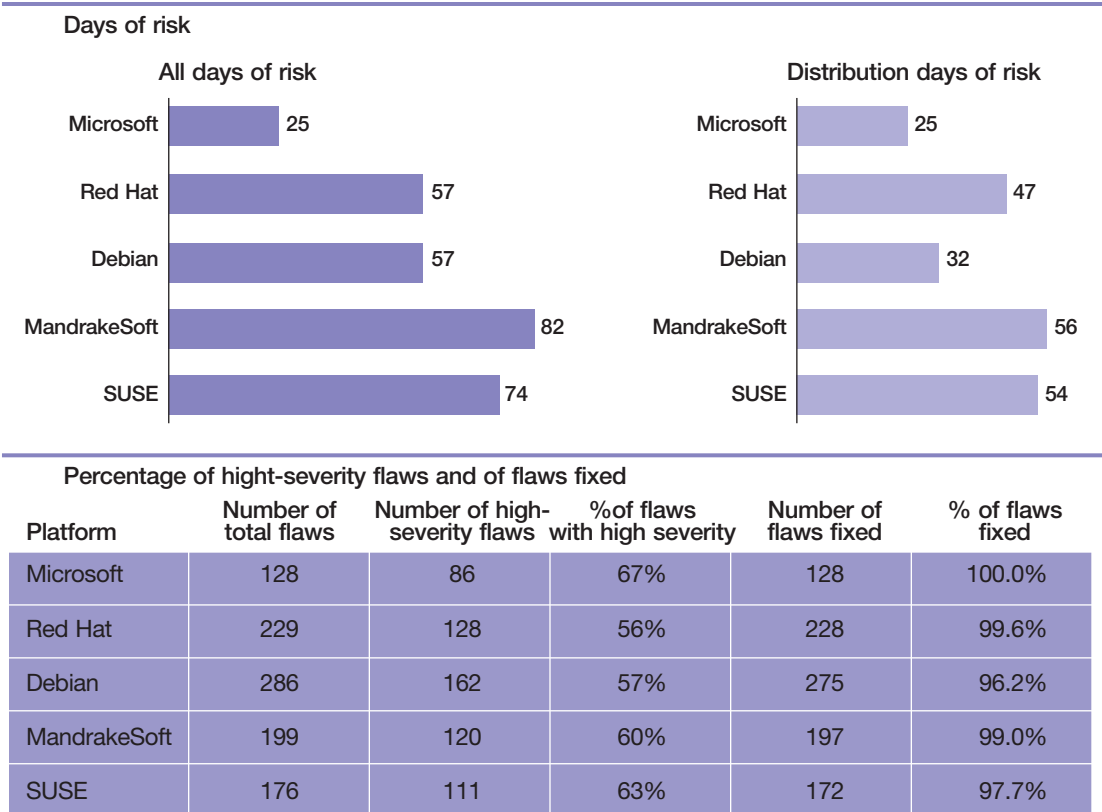
Note: In 2005, Microsoft will release a significant update to its software update services: Windows Update Services. This solution will bring enterprise-class patch management system capabilities to organizations of all sizes, but without the complexity or cost of most enterprise applications.

As the number of required patches for Microsoft products has decreased, both the speed of patch development and the quality of patches have increased. Microsoft has become so efficient in developing and releasing patches (after the company is aware of a vulnerability) that in March 2004, Forrester Research could demonstrate that Microsoft had the fewest days of risk compared with the major Linux distributions available on the market.

The study covered the 12-month period of June 1, 2002, through May 31, 2003. Researchers gathered metrics about the number of days from a problem's public disclosure to the OS vendor's released fix. For the timeframe Forrester Research analyzed in the study, Microsoft had an "all days of risk" rating of 25 days across all patches. The nearest competitor—RedHat Linux—had a rating of 57 days, and MandrakeSoft held the worst record at 82 days. The graphics in Figure 1-2 illustrate this quantification of platform security.

**Figure 1-2**  
*Quantifying platform security*

 A spreadsheet with additional data is available online.



Source: Forrester Research, Inc.

Note: You can download the Forrester Research report “Is Linux More Secure Than Windows” from <http://download.microsoft.com/download/9/c/7/9c793b76-9eec-4081-98ef-f1d0ebfffe9d/linux/windowssecurity.pdf>.

Microsoft’s gains in getting patches out fast are significant enough on their own, but coupled with the decreased number of necessary security patches and the tools available to easily deploy patches, *secure in deployment* is an increasingly obtainable goal.

Finally, no amount of improvement in getting patches out and making them easy to deploy would be complete without one final principle—communication. After all, the patch you need at the moment you need it doesn’t do you any good if you don’t know about it! To communicate with as wide an audience as possible, Microsoft has improved its timeliness in releasing vulnerability information—and the company offers an exceptional level of detail about which types of systems require each patch, which files the patch changes, and more.

## The First Step to Security: Understanding

In the light of Microsoft's progress in making Windows as secure an OS as possible (with more improvements to come), I'll explore the types of threats that most organizations are likely to face. Studying potential threats lets you better understand what's behind them and how to protect your systems from them now and in the future.

Security threats to your network come from two possible locations—from the outside world and from within the organization. In the first case, threats come from individuals or systems that aren't part of your organization and therefore have no authorization to use any system in your network. This threat source is the one most people think about instinctively when they consider security.

### *Threats from Outside*

Whether it's a virus attachment in an email message, an Internet worm attempting to propagate itself, attempted unauthorized access to your data, or a Denial of Service (DoS) attack against your systems—external entry attempts comprise the majority of the security threats facing most organizations today. To ensure a common understanding of these threats, I offer a few definitions.

**Virus**—A program or piece of code that's loaded onto your computer without your knowledge or consent. A virus can exist by itself or attach itself to an executable file or to document files that have scripting capabilities. Viruses typically need some sort of user intervention to execute and infect a system. Viruses can replicate themselves.

**Worm**—A program or algorithm that replicates itself over a network of computers (e.g., the Internet) and performs some sort of malicious action, such as defacing a Web page. Unlike a virus, a worm requires no user intervention to infect a system. If it finds a vulnerable system, that system is instantly infected.

**DoS**—A type of attack on a network that's designed to bring the network to its knees by flooding servers, routers, or other devices with useless traffic, or causing them to exhaust all of their resources through other mechanisms. In either case, the result is the same—the network, or portions of it, becomes unusable.

### *Defense in Depth*

The best strategy to mitigate these threats is the use of multiple layers of security, commonly referred to as *defense in depth*. Taking a page from the US Department of Defense (DOD), you can protect your system by “mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and allow the commander to maneuver his [or her] reserve.”

In the world of technology, this strategy could involve a number of measures—such as ACLs enabled on your routers that face the Internet, proper rule sets within your firewalls, a DMZ for any public-facing systems, effective Virtual LAN (VLAN) isolation on switches, the removal of unnecessary services from servers, hardened services, tight security controls on core OS files, and an auditing policy enforced throughout the network.

A layered approach can help you build much stronger defenses around your organization's network. Unfortunately, too many administrators use the opposite approach. They place the lion's share of the burden of securing the network on a single border device such as a firewall, and they do nothing else. In the security world, administrators refer to the system that this single-device approach creates as being “crunchy on the outside, with a soft, chewy center.” Such implementations let worms

(e.g., Code Red) propagate—because the payload for that attack, which came as a part of an HTTP request, slipped past nearly every firewall in the world. I'll discuss approaches to security in depth in the chapters that follow.

### ***Additional Defenses Against Attack Techniques***

To supplement the defense-in-depth model, you need to know which techniques intruders might use if they were to specifically target *your* organization's network for some reason. Such intruders tend to follow a very methodical approach to compromising your network, and they're often quite patient in doing so. To better understand how intruders work, take a moment to try to think as they might think—with the help of the material that follows, drawn from Joel Scambray and Stuart McClure's *Hacking Windows 2000 Exposed* (Osborne/McGraw-Hill, 2001). Intruders typically employ the following techniques when they attempt to compromise a network.

### **Footprinting**

In this real-world equivalent of “casing the establishment,” no packets have yet been transmitted to your network. Instead, intruders research everything they can find out about your organization—perhaps by using something as simple as a business card as a starting point. Let's look at the fictitious business card (image courtesy of iPrint.com) that Figure 1-3 shows.

**Figure 1-3**  
*Business card—an intruder's view*



From a business card, intruders can discover a number of useful things—such as the physical location of the organization, its email domain name, the format that its email addresses typically follow, and a block of phone numbers the organization uses. Once intruders know the domain name, they can discover who registered that domain (the name and email address) for a possible social engineering attack. (In such an attack, an email message appears to have come from a sender the recipient trusts, making it more likely that the email message will pass through filters and less likely that the recipient will view it with suspicion.)

Additionally, it's not much of a challenge to discover which servers process the company's email and what those servers' IP addresses are. Finding the IP address of the company's Web site is also trivial. The intruder can gain some network blocks with which to start. From the *dtoombs@* email address format, intruders might well guess the company's logon naming convention as well because many organizations follow a standard of first initial+last name (or something similar).

This collected information gives intruders 50 percent of the credentials they need to access your network. Add the fact that one can often find the names and email addresses of top executives on company Web sites, and the intruders have multiple names at their disposal. At this point, intruders haven't yet done anything illegal, but they're well on their way to mounting an attack on your network.

## Scanning

After intruders figure out some of the IP addresses an organization uses, scanning helps them find all of the devices available within the network. They use various ping scans and other query mechanisms. After intruders complete the scanning, they identify the hosts they'll target for enumeration. At this point, the intruders are definitely transmitting packets into your network.

Note: In many countries, it isn't clear whether scanning is illegal. Although most security experts would say that scanning is illegal in the United States, a glance at the section titled Federal Criminal Code Related to Computer Intrusions on the following Web site indicates the complexities involved: <http://www.cybercrime.gov/cclaws.html>.

## Enumeration

When you know which hosts or devices are part of a company's network, enumerating services running on the hosts is relatively simple. You can readily find port scanners that are designed to determine which services are listening on which ports. Having that information lets intruders plan a custom attack based on known vulnerabilities in certain applications. Although it's questionable whether enumeration is illegal, the act of enumeration makes the intruder's intent to penetrate your system more obvious.

## Penetration

As the attack preparation escalates, intruders will attempt to gain access to a low-privilege account within your organization. They might do so by attacking your network directly (which is illegal, per United States Code, Title 18, Chapter 47, 1030) or indirectly, by using a social engineering attack. An intruder might attempt to call your Help desk and pose as a user who needs his or her password reset. (The intruder might pose as someone whose business card he or she has acquired or someone listed in the domain registration records.)

If you don't think intruders could find out your Help desk's phone number, try this exercise (if your organization is large enough). Call your organization's main phone number and get the switchboard operator. Ask for the mailroom. When the operator switches you over, claim that you were trying to dial the Help desk and simply misdialed. Ask the mailroom clerk to transfer you to the Help desk. Many will gladly do so.

## Escalation

After intruders compromise a low-privilege account, they'll attempt to escalate that account to a higher level of privilege—ultimately aiming to have administrative authority within the network. If

intruders successfully achieve administrative privileges, it's only a short matter of time before they complete the final steps of penetrating your network.

### Getting Local

If intruders have successfully entered a system, they've reached one—usually only the first—of their goals. They can then continue to the goal of compromising the server's LocalSystem security context—the most trusted context on any Windows host. The OS won't see commands as coming from a trusted administrator, but think that it (the OS) is issuing its own commands.

### Expanding Influence

Why own one system when you can own them all? Obviously, if intruders gain a successful foothold within your network, they'll attempt to expand that foothold until they achieve their ultimate goal. If that goal is to take over your entire network, they'll target one system at a time until they do so. However, if the goal is to target data known to be on a specific server (e.g., payroll data, medical data, credit card information), they'll expand their influence to reach their goal with a minimal amount of work.

### Cleanup

To stay under the radar, intruders will cover their tracks whenever possible. Their cleanup process will include clearing event logs or removing specific items from them. The longer they can stay off the radar, the longer they can influence your network exactly as they want to.

I hope that by trying to think like intruders and understand how they work, you can better defend your network against those attempting to get in. I'll discuss the threats from outside and how to protect yourself from them in much more detail in the chapters that follow.

### Threats from Inside

As if threats from the outside world weren't enough, today's administrators must face an entirely new class of threats—from the inside. Internal dangers include threats that trusted users (knowingly or unknowingly) bring into your network. Just like school kids who bring home stomach flu germs, these users don't intend to harm the organization's network. Most of them would take additional precautions to avoid doing so if asked. Nevertheless, they threaten your network. (I say that *most* users would take additional precautions to protect the organization's network because a few users will unfortunately think that certain requests are unreasonable or that compliance will affect them too much.)

### A Case in Point

A small law firm with which I consulted needed two desktop PCs for two secretaries who sat in one office. Both secretaries had been with the law firm for roughly the same period of time, so both were completely familiar with Windows, Microsoft Office, and other applications that they needed to accomplish their work.

About 6 months after I delivered and installed the two PCs, the firm called me about a performance problem on one of the PCs. What became clear was that one secretary was content to use Microsoft Word to work with her documents, keep the books in the firm's accounting system, and do little else through the PC. The other, however, had installed AOL on her PC, and she must have clicked and executed every attachment she received. Her system was infested with buggy applications and DLLs and had slowed to a crawl.

After a few hours of cleanup and a strong admonishment about the dangers of launching email message attachments (other than documents and photos), I was on my way. However, 2 weeks later, her computer was completely wiped out by a virus—destroying a considerable amount of data that had been stored on her hard drive.

Although she was subsequently fired, she never felt that launching applications sent through email would do any harm—even after specifically being told that they could. Although this woman’s intentions were harmless, her actions were costly.

But what about the individuals in your organization whose intentions *aren’t* harmless? Much like the woman who embezzled nearly a million dollars from North Bay Health Care Group, some employees will actively seek to do you harm. They’ll try to use their status as trusted employees to manipulate data they shouldn’t access, to embezzle funds, or to disrupt systems.

Organizations must assume that they might have users who unintentionally or intentionally pose a threat from the inside (trusted) world. A threat might come from users who install AOL and read their email messages from their PCs, use a Web-based email service, or unknowingly install spyware. However, a threat might also come from users who alter data in your accounting system to issue checks to themselves. The threat from the inside world has always been a significant one, and it has grown in recent years.

## A Secure Windows Network

From 1999 through 2001, I designed secure Windows installations and networks for clients. Not a single system among them was compromised by Code Red or Nimda. At that time, I believed that with proper implementation you could have a secure Windows installation. Despite the mainstream media’s assertions to the contrary, I knew it could be done—because I did it. Today, I still firmly believe that you can have a secure Windows network and that achieving it is easier than ever before.

## A Secure Microsoft Network

In the chapters that follow, I’ll divide the security puzzle into two roughly equal halves. I’ll first take several chapters to cover threats from the outside world, where most of today’s threats originate. I’ll then explore the threats from the inside that organizations face. Each threat involves a unique set of concerns you should understand. After I cover those concerns, I’ll explore approaches you can use to address that threat.

I’ll discuss how you can apply the principles of the defense-in-depth approach when you design your systems. I’ll also make sure you’re aware of the features and tools that Trustworthy Computing offers to make your systems more secure and easier to patch during their expected life cycle. Where existing products can increase your network’s security, I’ll describe how to implement them. And I’ll consider security products just coming into the market. A secure Microsoft network isn’t a myth. With the right tools, anyone willing to put time into creating such a network can have one.

## Next: Hardening Your Network

Chapter 2 will specifically discuss how hardening your network can help protect your system from outside threats. I’ll discuss how to build a proper DMZ. I’ll then cover Microsoft Internet Security and Acceleration (ISA) Server in depth, in conjunction with using firewalls and VPN remote access. And more!