CHAPTER 1

Understanding Core Security Principles

Every computer presents a certain level of risk. You can't eliminate risk unless you simply never turn on the computer. However, you can manage risk. You start by understanding what risk is and understanding that risk mitigation is accomplished by reducing vulnerabilities.

Several core security principles guide the protection of information technology (IT) systems and data. When you understand these core security principles, it's easier to grasp the reasoning behind many of the security practices.

Most security principles can be traced back to the *security triad* (also called the AIC or CIA triad). The security triad mandates protection against the loss of confidentiality, the loss of integrity, and the loss of availability of IT systems and data. Other principles include defense-in-depth and the principle of least privilege. Administrators *harden*, or secure, IT systems by attempting to configure them more securely than the default configuration and reduce vulnerabilities. This chapter covers all of these topics in the following sections:

- **Understanding risk**
- **Exploring the security triad**
- **Implementing a defense-in-depth security strategy**
- **Enforcing the principle of least privilege**
- **Hardening a server**

Understanding Risk

Minimizing risk is also known as *risk mitigation*.

Risk is unavoidable. You can't eliminate it. However, it's possible to minimize risk by first understanding it and then taking steps to mitigate it.

For example, every time you step into a street, you run the risk of being hit by a car. The real threat of a car colliding with your body, and your body's

vulnerability to this collision, convinces you to take steps to reduce the risk. Unless you're Superman, you can't stop the threat. If the car is coming, it's coming. But you can minimize the risk by using crosswalks and looking for approaching cars before stepping into the street.

The next section explains the concepts of confidentiality, integrity, and availability in more depth.

Similarly, risks are reduced in IT networks by taking steps to reduce the vulnerabilities. Consider Figure 1.1. Risk occurs when *threats* exploit *vulnerabilities*. In an IT environment, threats are any events that can result in the loss of *confidentiality*, *integrity*, or *availability* of IT systems or data. Threats can be man-made or natural.

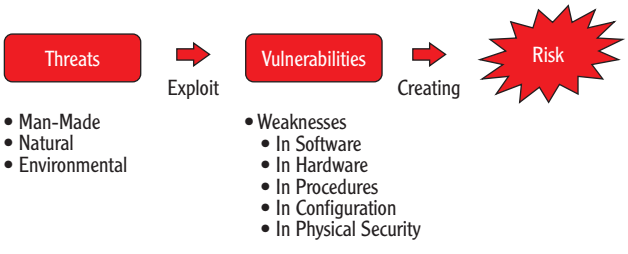


FIGURE 1.1 **Threats exploit vulnerabilities, creating risk.**

NIST's Definition of Risk

The National Institute of Standards and Technology (NIST) is a U.S. agency that includes the Information Technology Laboratory (ITL). The ITL regularly conducts research and publishes papers on behalf of NIST.

Much of NIST's research focuses on what the U.S. government can do to improve security for its IT systems and data. However, these papers are publically available, and many non-government organizations adopt the techniques and methodologies.

NIST's Special Publication 800-30 (SP 800-30) is titled "Risk Management Guide for Information Technology Systems." The definition of *risk* in SP 800-30 is as follows: "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." Although you don't need to memorize this quote, it's worth noting that it does add more depth than just *Risk occurs when a threat exploits a vulnerability*.

Risk management is a complex topic that includes multiple facets. At this stage of your study, you don't need to master all the different topics of risk management, but you should be aware that much more detail is available.

(Continues)

NIST's Definition of Risk *(Continued)*

If the topic appeals to you, you can use the Microsoft Technology Associate Security Fundamentals certification as a springboard to more advanced security certifications such as ISC(2)s Certified Information Systems Security Professional (CISSP) certification.

Man-made threats are any threats from people. These can be intentional threats such as attacks or malware distribution. Intentional threats can also include the access, modification, or deletion of data. Other threats include theft, fire, and vandalism. Man-made threats can also be unintentional, such as the accidental deletion of data. Natural threats include weather events such as hurricanes, floods, tornadoes, and lightning. Environmental threats include long-term power failures or the inadvertent release of hazardous chemicals.

An important point to keep in mind is that you can't stop threats. If someone wants to write malicious software, you can't prevent it. If Mother Nature wants to create a tornado, it's coming. However, you can reduce risks by reducing vulnerabilities.

Vulnerabilities are weaknesses. These can be inherent weaknesses in your software or hardware, such as bugs in the code or faulty power supplies. They can be weaknesses in procedures that allow users to give up valuable data to social engineers. They can be weaknesses in security configurations, such as when unneeded services or protocols are left running on a system. They can be weaknesses in physical security that allow unauthorized personnel access to servers or network devices.

Reducing vulnerabilities is the core of risk management in an IT environment. Every step you take to reduce weaknesses reduces your risks. The following list identifies some common techniques you can use to reduce weaknesses. Don't worry if you don't understand them all right now—they're covered in more depth throughout this book:

- Enforce the principle of least privilege.
- Implement strong authentication mechanisms.
- Train employees on risks of social engineering.
- Regularly remind employees about their security responsibilities.
- Implement multiple layers of security (defense-in-depth).
- Remove or disable unneeded services and protocols.

- Implement host-based and network-based firewalls.
- Keep all systems up to date with patches.
- Install and update antivirus software.
- Add redundancies for critical systems.
- Secure access to data with permissions.
- Back up data and store a backup copy off-site.
- Track access to data and systems with audit trails.
- Encrypt critical data at rest and when transmitted on the wire.
- Protect systems, data, and facilities with strong physical security.

Although this book isn't a comprehensive source for mitigating all risks, it does include basic information you can use as a foundation.

Exploring the Security Triad

The security triad includes three key security principles that are at the core of all security practices. These are sometimes called the AIC triad or the CIA triad, using the first initials of each (*availability*, *integrity*, and *confidentiality*).

Any study of IT security requires an understanding of these basic principles. Figure 1.2 shows the three elements in the security triad. These three elements combine to provide a solid layer of protection for assets within an organization:

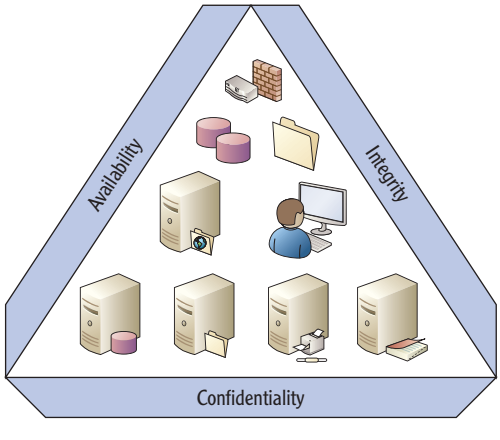


FIGURE 1.2 Security triad

Confidentiality This element ensures that only authorized people are able to access data.

Availability Availability ensures that systems and data are up and available when needed.

Integrity Data integrity prevents the unauthorized modification of data and ensures that unauthorized modification is detected.

Protecting Against Loss of Confidentiality

The loss of confidentiality occurs when unauthorized individuals access data. A company needs to keep its secrets secret. If unauthorized people can access the secrets, they just aren't secret any more.

You can take several steps to ensure confidentiality. You start by ensuring that everyone who accesses data is authenticated. In other words, users log onto a system with a username and password or another authentication method.

You then use access-control methods to control who can access the data. For example, you can assign permissions to specific files and folders. If a user doesn't need access, they aren't granted permissions.

Encryption is another layer of security to protect against the loss of confidentiality. You can encrypt individual files, entire hard drives, and data transmissions traveling across the network. If an individual does obtain an encrypted file, it's scrambled in such a way that it's unreadable until it's decrypted. Strong encryption standards ensure that unauthorized individuals aren't able to decrypt any encrypted data.

Protecting Against Loss of Availability

Loss of availability simply means that systems or data aren't available when the user needs them. Some systems need to be up and operational 24 hours a day, 7 days a week, such as web servers available on the Internet. Other systems only need to be available from 9 a.m. to 5 p.m. Monday through Friday, such as computers used by employees during the day.

You ensure that systems stay operational by protecting against different threats and building in redundancies. One of the most common threats to systems today comes from malicious software (malware). *Malware* includes viruses, worms, Trojan horses, and more.

Backups are important to consider. If you've never lost any data, you're luckier than most. However, it's just a matter of time. You'll lose data. And when you do, the difference between a major catastrophe and a minor inconvenience is the existence of a backup. If you have a copy of your data, you can simply restore it, and you're back in business. If you don't have a copy, you'll have to rebuild the data from scratch.

Chapter 3 covers authentication in more depth, including the three factors of authentication: something you know, something you have, and something you are.

Chapter 4 explains the different types of permissions in a Microsoft network. In that chapter, you'll learn how to secure access to data with permissions.

Chapter 10 explains the different types of encryption that are available to enforce confidentiality in Microsoft networks.

Chapter 2 presents the different types of malware and methods to protect against it. You'll also learn about threats from social engineering.

Organizations keep a copy of backups in a separate geographical location, such as a separate building. This ensures that the organization can recover from a major catastrophe such as a fire.

Organizations implement sophisticated backup plans to ensure that they have copies of all their important data. Additionally, organizations with mature backup plans maintain a copy of data off-site.

Fault-tolerant or redundant technologies can be built into systems at multiple levels. A fault-tolerant system ensures continued operation even if a failure, or fault, occurs. Redundant Arrays of Independent Disks (RAIDs) provide fault tolerance for hard drives. Failover clusters provide fault tolerance for servers. Hot, warm, or cold sites provide fault tolerance for entire locations.

Of course, not every business has an alternate location. Similarly, not every system and every drive includes fault tolerance. The organization determines what to implement based on the value of the systems and data and the cost to protect them.

Protecting Against Loss of Integrity

The loss of integrity occurs when data is modified without authorization. This can occur if unauthorized individuals modify data.

Chapter 5 covers audit policies and network auditing. You'll learn about what can be audited in a Microsoft network.

Access controls work to ensure that only authorized people have access. However, malicious users may bypass the controls, or the controls may fail. Audit logging can show if anyone accessed data and may include details such as who they are, what they did, and when they did it.

In addition to auditing, hashing detects when data has lost integrity. In its simplest form, a *hash* is simply a number. A *hashing algorithm* is a mathematical calculation that you can execute against a file or a message to create the hash, or the number. As long as the data stays the same, a hashing algorithm will always produce the same hash (or the same number). If the data changes, the hashing algorithm will produce a different hash indicating the data has changed.

Hashes are created at a given time to identify the original state of the data. They're then re-created at a later time to see if the hash has changed. If the two hashes are different, the data has lost data integrity. However, if the two hashes are the same, the data has maintained integrity.

Chapter 10 includes information on how email can be digitally signed to provide both authentication and integrity.

As a simple example, a message may have a hash of 12345 when a user creates and sends it. The sending computer sends both the message and the calculated hash. Another computer receives the message and calculates the hash again. If the recalculated hash is 12345, the receiving computer knows the message hasn't been modified. It hasn't lost data integrity. However, if the recalculated hash is 98765, the receiving computer will recognize that this is different from the original hash of 12345. Because the hashes are different, the data is different. The data has lost its integrity.

Many organizations implement a Public Key Infrastructure (PKI) so that they can issue their own certificates. For example, a PKI can issue certificates to users to digitally sign email and ensure integrity.

Chapter 11 presents information on a Public Key Infrastructure and digital certificates.

Implementing a Defense-in-Depth Security Strategy

Defense-in-depth is a strategy employed by security professionals that includes multiple layers of security. Instead of implementing one security technique and then celebrating success, you must treat security as an ongoing process. You can't simply password protect your systems and files and say you're done.

Think about an attacker. Attackers often get money when they successfully attack a network. Sure, some attackers are just thrill seekers hacking into a system for the fun of it. But most attackers today are dedicated criminals trying to break into systems for monetary gain.

Imagine that an attacker can make $5,000 a week from attacks. He is likely highly motivated to learn everything he can about security procedures and methods. Moreover, he knows how to break into networks and systems to get the information he needs. If you employ just a single security procedure that he's already cracked, his job is easy. However, if instead you employ multiple layers of security, he must know how to break each one. It takes time and effort to break down each layer.

Defense-in-depth strategies often slow down or deter an attacker. This delay can provide extra time to detect the attack and respond to it.

Defense-in-depth strategies defend against threats at multiple points and at multiple layers. They use a combination of policies, operations procedures, people, and security technologies. Figure 1.3 outlines many of the elements of a defense-in-depth strategy and identifies the chapters where these topics are covered.

Notice that policies and procedures represent a first line of defense. Behind that is physical security, which provides a second line of defense. Then, within each of the technical topics (such as data, auditing, and so on), multiple security methods are employed to provide additional layers of protection. The lines of defense and security methods outlined here aren't all-inclusive, but they do cover many of the typical security measures used to protect IT infrastructures:

Administrative Policies and Procedures These are written rules that outline security requirements. They let administrators know what security to implement, and they let users in the organization know what is expected of them. These often include steps to maintain a high level of security awareness by all users. For example, users may be reminded of the dangers of malicious software (malware) and about current social

Chapter 2 presents information on malware and social engineering. Chapter 3 covers the different methods of authentication.

engineering tactics employed by attackers. Acceptable methods of authentication are also outlined as part of a basic access policy.

Defense-in-depth also provides protection if one layer of security fails. Even if one fails, other layers remain in place.

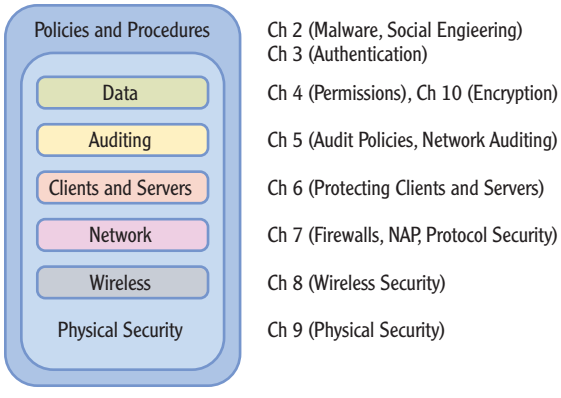


FIGURE 1.3 Defense-in-depth strategies, and the corresponding chapters in this book

Chapter 4 covers NTFS, share, registry, and Active Directory permissions in more depth.

Data You can protect data with permissions and encryption. Files, folders, and shares are secured with New Technology File System (NTFS) permissions and share permissions. Other permissions include registry permissions and Active Directory permissions.

Chapter 5 covers audit policies and methods for auditing a network for security compliance.

Auditing Auditing is the process of tracking access. It identifies what was done, when it was done, where it was done, and who did it. For example, you may have proprietary data and want to track all access to it. You can enable auditing to create an ongoing audit trail that will show which users have accessed the content, when they accessed it, and what actions they performed.

Chapter 6 goes into more depth on protecting clients and servers.

Clients and Servers Clients and servers within a network must be secured. At the most basic level, antivirus software protects these systems from malware. Additionally, systems must be kept updated with current security patches and hotfixes.

Network Almost all data used in organizations today travels through the network at one time or other. Attackers can use tools such as sniffers to capture and analyze data traveling through a network if it isn't secure. Securing a network includes using tools such as firewalls to control the traffic, or Network Access Protection (NAP) to control the clients accessing the network. You can also encrypt critical data using Internet Protocol Security (IPSec).

Chapter 7 covers firewalls, NAP, and protocol security.

Wireless Wireless networks are very valuable, allowing you to quickly set up a network without running cables to every system. However, wireless traffic can easily be intercepted, so wireless networks require additional steps to secure. Whereas early wireless networks were highly insecure, today there are protocols and methods you can use to provide a higher level of security.

Physical Security This uses locked doors and other physical security measures to protect assets. For example, servers and network devices are often locked in server rooms or wiring closets, and only a limited number of people have access.

Chapter 8 covers wireless security, including WEP, WPA and WPA2.

Chapter 9 covers physical security, including the use of technical policies to restrict the use of removable devices and drives.

Enforcing the Principle of Least Privilege

Another core security principle is the principle of least privilege. Users, resources, and applications should be given the rights and permissions to perform necessary tasks, and nothing else.

For example, if users need access to project data on a computer, they should be given minimal access to that data. A gross violation of the principle is to give these users full administrator access. Yes, they will be able to access the project data with administrator access, but they can also do anything else on the computer. Some administrators may be tempted to give everyone administrator access instead of managing the permissions. Admittedly, this is easier in the short term. However, people can accidentally cause problems. They can access data they shouldn't see (like other employees' pay data), and some may even maliciously delete or modify the data. When the incidents start, it'll take a lot of time and energy to get things back in order, and some of the damage may be irreversible.

Malware and Least Privilege

When malware infects a computer, it attempts to escalate its privileges to the highest level possible. If a user has administrative privileges on a system, the malware can usually escalate its privileges to the same level. However, if a principle of least privilege is used, few users will have administrative permissions. Therefore, the possibility of malware escalating its privileges is reduced.

Many organizations issue administrators two accounts: one account is used for regular work, and the second account is used for administrative work. Administrators only use the administrator account when doing administrative work. The administrator will typically be logged on with their regular account the majority of the time.

This reduces the risk of malware escalating its privileges to the administrator level. Note that by itself, this doesn't prevent a system from becoming infected; that's done with a strong anti-malware program. But if an administrator uses the administrator account only 10 percent of the work time, this reduces the likelihood of a system becoming infected and subsequently the malware from obtaining administrator access.

A *service account* is an account used to start a service or application. Service accounts can be built-in accounts, local accounts, or domain-level accounts.

Additionally, any accounts that are created for service accounts should also use the principle of least privilege. These service accounts should be granted the minimal necessary rights and permissions for the service or application to run as needed.

As an example, Figure 1.4 shows the Log On tab of the DNS Server service properties page. Each time the DNS server starts, it uses the Local System account to access any resources. Notice that you have the capability to change this setting to This Account and add an account name and password to start the service (including the administrator account), but this isn't necessary for the DNS Server service. The minimal access that the DNS Server service requires is local access from the Local System account.

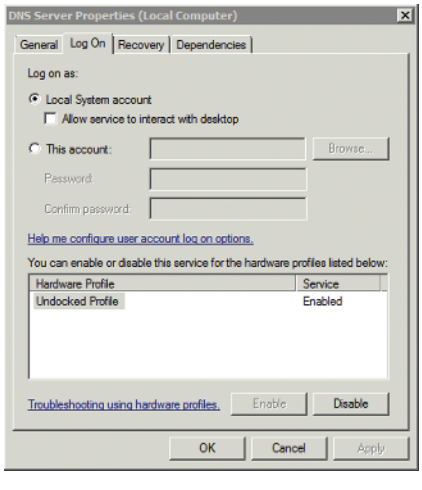


FIGURE 1.4 DNS Server service Log On settings

Hardening a Server

Hardening a server indicates that you're making changes to the default configuration in order to enhance the system's security. You can take multiple steps to harden a server. These include the following:

- Reduce the attack surface.
- Keep the operating system up to date.

- Enable firewalls.
- Install and update antivirus software.

The following sections explore these steps in more depth.

Reducing the Attack Surface

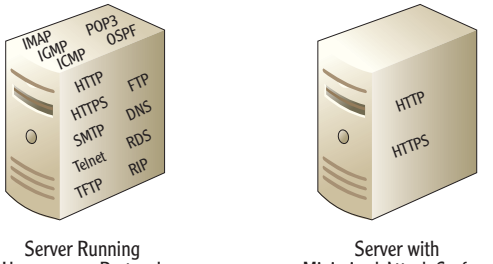
You *reduce the attack surface* of a computer by ensuring that only necessary services and protocols are running or installed on the system. If a protocol isn't installed on a system, it can't be attacked.

As an example, consider a web server. It's primary purpose is to host web pages that users access over the Internet or intranet. A web server uses Hypertext Transfer Protocol (HTTP) and HTTP with Secure Socket Layers (HTTPS) as the protocols to serve these web pages. On the server, HTTP and HTTPS are required and must be running in order to present users with both plain text and secure web pages. However, other protocols such as Telnet and the Simple Mail Transport Protocol (SMTP) aren't needed.

Some web servers use SMTP. Of course, if SMTP is required by the website, it's a necessary protocol. In our example, SMTP isn't needed.

If the Telnet Server service is running, it may be possible for an attacker to connect into the server using Telnet and launch an attack. However, if the Telnet Server service is disabled, a Telnet attack isn't possible. Similarly, if SMTP is installed and running, the system is susceptible to possible attacks that exploit vulnerabilities in SMTP. Remove SMTP, and all SMTP attacks are blocked.

Figure 1.5 shows two web servers. The server on the left is running several additional unneeded protocols. These additional protocols are all subject to attack. The server on the right is much more secure simply by having the unnecessary services and protocols removed or disabled.



A server with a reduced attack surface is still subject to attack. However, there are fewer attack possibilities.

FIGURE 1.5 **Minimizing the attack surface of a server**

There's an added benefit to reducing the attack surface. If there are fewer protocols running on a system, there is less to manage. The administrator only needs to focus on the installed protocols. Unfortunately, when all the extra protocols are running,

administrators sometimes still focus only on the required protocols. In other words, the administrator may simply forget about these extra protocols and not manage or monitor them. Attacks may go unnoticed until the damage is catastrophic.

Although it's simple to say that unnecessary services and protocols should be disabled and removed, it's not as easy to identify which are necessary and which aren't. However, there are tools that can help. For example, the Security Configuration Wizard (SCW) is built into Microsoft Windows Server 2008 and Microsoft Windows Server 2008 R2. It can analyze a system and recommend more secure settings for services, firewall rules, the registry, audit policies, and more. Figure 1.6 shows one screen of the SCW where the wizard is recommending changes to the startup mode of different services.

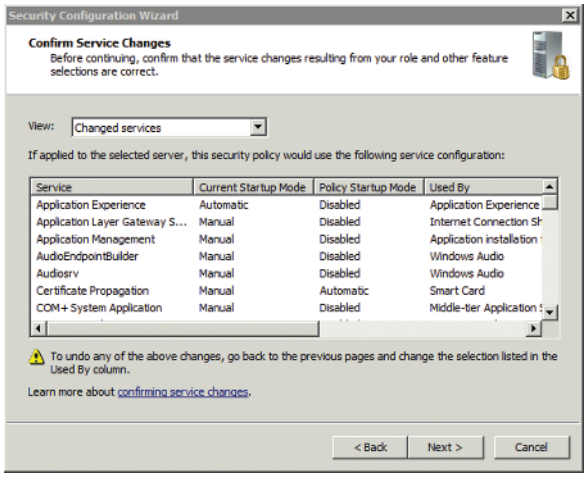


FIGURE 1.6 Security Configuration Wizard service startup mode recommendations

You can launch the SCW on a Windows Server 2008 system by choosing Start ➢ Administrative Tools, and selecting Security Configuration Wizard. The wizard leads you through several screens, allowing you to create, edit, apply, and roll back settings for security policies.

The following steps show how to create a security policy on a Windows Server 2008 server using the SCW:

1. Choose Start ➢ Administrative Tools, and select Security Configuration Wizard.
2. Review the information on each of the screens. Click Next to accept the defaults on each of the screens until you reach the Security Policy File Name page.

3. On the Security Policy File Name page, enter a name of Test at the end of the line. It will have this full path:

   ```
   C:\Windows\security\msscw\Policies\Test
   ```

   Click Next.

4. Ensure that Apply Later is selected on the Apply Security Policy page, and click Next.

5. Click Finish.

6. Launch Windows Explorer by clicking Start and selecting Computer.

7. Browse to `C:\Windows\security\msscw\Policies\Test`, and open the `test.xml` file you just created by double-clicking it. Your display will look similar to Figure 1.7.

SCW saves this as an Extensible Markup Language (XML) file. You can open XML files in many applications, including Internet Explorer and Notepad.

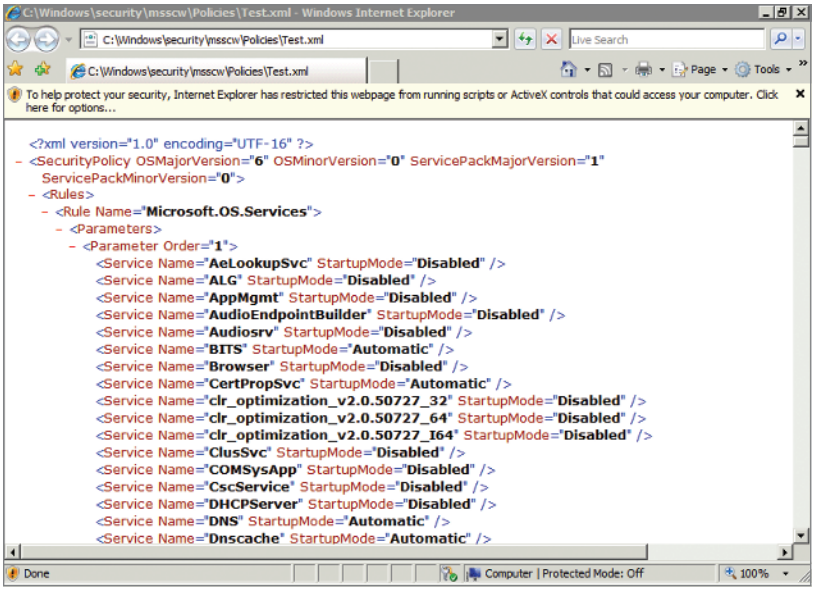


FIGURE 1.7 Security Configuration Wizard security policy shown in Internet Explorer

8. Scroll through the security policy file to view the settings. As you can see, the policy is extensive. It includes several primary nodes, including the following:

   - Microsoft.OS.Services (to secure the services)
   - Microsoft.OS.Networking.Firewall (to implement firewall rules)

- Microsoft.OS.Registry.Values (to secure the registry)
- Microsoft.OS.Audit (to enable auditing)

You can copy this `.xml` file to another computer and apply it. For example, if you have five identical web servers in a web farm, you can create one security policy, test it, and then apply it equally to all the servers.

It's often useful to create a policy using the SCW, but sometimes you may want to focus on a specific server role to determine what the most secure settings are. The SCW includes an extensive database that you can browse for different security settings. Figure 1.8 shows the entry page of this database. It includes security settings for just about all the possible server roles, client features, administration options, service settings, and Windows Firewall settings. You can view this page by clicking the View Configuration Database button on the fourth page in the SCW.

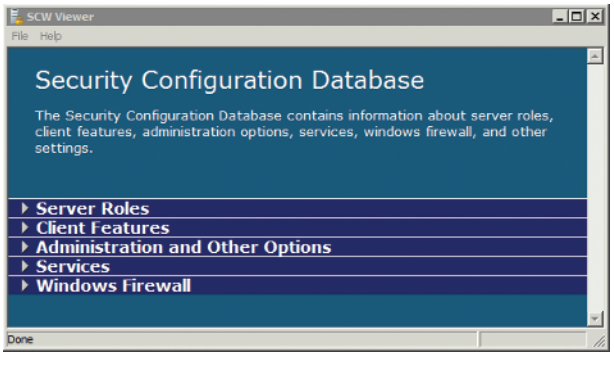


FIGURE 1.8 Security Configuration Database viewed from the SCW

Some high-profile security patches are released out-of-band. If a security threat is high and immediate, Microsoft sometimes releases the patch earlier than the second Tuesday of the month.

Keeping a System Updated

Operating system software is often insecure. That may sound like a strong statement, but it's true. As long as you're using a computer, there are operating system vulnerabilities that can be exploited. The trick is to discover the known vulnerabilities and fix them as quickly as possible.

Microsoft routinely investigates bugs and flaws in released operating systems. The company regularly writes and releases patches and hotfixes to correct the problems. A *patch*, or *hotfix*, is a small amount of code that corrects a problem.

Microsoft releases security updates on the second Tuesday of every month, known as *Patch Tuesday*. Because administrators know when patches will be released, they can plan for them and manage their deployment.

Many organizations use Automatic Update to automatically install the updates when they're released. Unfortunately, sometimes a patch that is intended to fix one problem may create another. For example, a security update may address a known security issue, but an unwanted side effect of the update may be to prevent an application from running. If one computer stops working, it's inconvenient. However, if all 500 computers in an organization suddenly stop working, it can be catastrophic.

Organizations often use a tool such as Windows Server Update Services (WSUS) or Microsoft System Center Configuration Manager (SCCM) to manage the deployment of updates.

Both WSUS and SCCM allow administrators to test updates before deploying them. Updates that create conflict with existing computer configurations aren't deployed. Other updates can be easily deployed to all systems in the organization. It doesn't matter if the organization has 50 computers, 5,000, or more; a few clicks send the update to all of the targeted computers.

WSUS is a free product available on Microsoft's download site. SCCM is an add-on server product. SCCM has more capabilities than WSUS.

One benefit of SCCM over WSUS is that SCCM supports scheduling. In other words, an administrator can schedule updates to deploy at certain times.

All Operating System Software Has Vulnerabilities

Because you hear about Microsoft systems being attacked and exploited, you may think they're the only operating systems that have security issues. Some people believe it so much that they repeat it. For example, some people say that Macs are so secure that antivirus software and updating aren't needed. Not true.

For example, in November 2010, *Computerworld* published an article titled "Apple Smashes Patch Record with Gigantic Update" (`www.computerworld.com/s/article/9196118/Apple_smashes_patch_record_with_gigantic_update`). It mentions that Apple fixed 134 flaws with Mac OS X. Mac OS X is based on a version of Unix known as Snow Leopard.

More than 90 percent of the systems in use are Microsoft based, so Microsoft systems get more press. This includes positive press demonstrating the power of these systems and negative press when vulnerabilities appear. If the most popular operating systems were produced by another company, you can bet these would have the most attacks and known security vulnerabilities.

Operating systems are very sophisticated and include billions of lines of code. Despite excellent programmers and extensive testing, bugs and flaws appear during the life cycle of any operating system. Many of these flaws are security related. Attackers can exploit them, and they do. The only way to ensure that an operating system stays as secure as possible is to keep it current with system updates.

Chapter 7 explores firewalls in more depth, including the Windows Firewall.

Enabling the Firewall

The Windows Firewall has been a part of Windows systems since Windows XP and Windows Server 2003. Since Windows XP Service Pack 2 (SP2) was first released, the Windows Firewall has been enabled by default. If you're using Windows Server 2008 or Windows Server 2008 R2, the Windows Firewall is enabled by default.

When you're hardening a server, it's important to ensure that a host firewall is enabled. Some companies purchase various third-party firewalls for use on their systems. However, the built-in Windows Firewall is natively installed and doesn't have any additional costs.

A host firewall is installed on the client or server. A network firewall is installed at a network boundary, such as between the Internet and an internal network.

Installing Antivirus Software

Every system that is on and accessible to people is susceptible to malware. Antivirus (AV) software can detect and block known malware, and it can often detect suspicious activities by unknown malware. Although malware is most often distributed through email, it can also be distributed through many other methods.

For example, if a user visits an infected website, the user's system can be infected. If a user inserts an infected USB into a system's USB port, the malware can install itself on the system. If a system is running on a network infected with a worm, the system can become infected.

Drive-by attacks download malware without the user's knowledge when the user visits a website. Chapter 12 covers Internet Explorer security that can protect users.

Every system should have AV software installed, although different systems need different protections. For example, the AV software installed on an email server is different from AV software you'd install on a database server or an end user's computer.

The Essentials and Beyond

This chapter introduced many of the basics related to IT security. Risk occurs when a threat has the potential to exploit a vulnerability, and risk mitigation reduces risks by reducing vulnerabilities. The security triad mandates the protection against loss of confidentiality, loss of integrity, and loss of availability of systems and data. A primary principle to protect against these losses is a defense-in-depth strategy, which includes multiple layers of security. Defense-in-depth increases the difficulty of exploiting systems and ensures that security remains in place even if one layer fails. The principle of least privilege states that users, resources, and applications are granted rights and permissions needed to perform their jobs, but no more. Last, hardening a server means making it more secure than the

(Continues)

The Essentials and Beyond *(Continued)*

default installation and includes performing actions that reduce the attack surface, keep it up to date, enable host firewalls, and use up-to-date antivirus software.

Additional Exercises

- Draw a diagram that shows the security triad.
- Run the Security Configuration Wizard on a Windows Server 2008 server. Identify the recommended state of the SMTP service (SMTPSVC) for the server's current configuration.
- Run the Security Configuration Wizard on a Windows Server 2008 server. Identify the recommended state of auditing for Logon events for the server's current configuration.
- Identify whether Windows Firewall is enabled on your system.

To compare your answers to the author's, please visit **`www.sybex.com/go/securityessentials`**.

Review Questions

1. What is a simple definition of risk?
2. True or false: You can reduce risk by reducing vulnerabilities.
3. An implementation of which security principle ensures that secrets stay secret?

   A. Authentication **C.** Integrity
   B. Availability **D.** Confidentiality

4. The implementation of techniques that map to which security principle help to ensure that an unauthorized change to data is detected?

   A. Accessibility **C.** Integrity
   B. Availability **D.** Confidentiality

5. A basic security principle states that users, resources, and applications should be granted only the rights and permissions needed to perform a task. What is this principle?
6. What is meant by *reducing the attack surface* of a system? (Choose all that apply.)

   A. Disabling needed services **C.** Keeping a system up to date
   B. Removing unneeded protocols **D.** Disabling the firewall

(Continues)

The Essentials and Beyond *(Continued)*

7. What tool can you use to create a comprehensive security policy as an XML file on a Windows Server 2008 system?

A. Microsoft Baseline Security Analyzer (MBSA)

B. System Center Configuration Manager (SCCM)

C. Security Configuration Wizard (SCW)

D. Windows Server Update Services (WSUS)

8. Of the following choices, what is the best method to protect against malware?

A. Installing antivirus software and keeping it up to date

B. Disabling unneeded services

C. Removing unnecessary protocols

D. Enabling a firewall