Network Security Policies & Procedures

by Sophia

WHAT'S COVERED

In this lesson, you will learn about the importance of security policies that provide a foundation for all network security. We will address a number of common considerations that should typically be incorporated into an enterprise security policy.

Specifically, this lesson will cover the following:

BEFORE YOU START

Every company should have written policies to effectively support the security of their computer networks. The policies should have the approval of the highest-ranking security or IT officer within the company, and they should address all aspects of the company network.

Procedures should also be in place to determine the appropriate course of action if there is a security breach. All network administrators and technicians need to be thoroughly trained in policies and procedures.

1. Security Policies

A **security policy** should define how security is to be implemented within an organization and include physical security, document security, and network security. For a policy to be effective, it has to be enforced consistently and completely. Nobody should be special enough to avoid adhering to it. And people have to understand the consequences of breaking policy too. Your network users need to have a clearly written document, called a security policy, that fully identifies and explains what is expected of them and what they can and cannot do on the network. People must be made completely aware of the consequences of breaking the rules, and penalties have to match the severity of the offense and be carried out quickly to be effective.

BIG IDEA

A written security policy document should serve as the foundation of the implementation of all technical security controls deployed in an enterprise computing environment.

The following terms and concepts are components that need to be considered in any network security plan.

TERM TO KNOW

Security Policy

A document that defines what it means to be secure for systems and networks within a particular organization.

1a. Security Audit

A **security audit** is a thorough examination of your network that includes testing all its components and security controls to make sure everything is secure. You can do this internally, but you can also contract an audit with a third party if you want the level of security to be certified. A valid and verified consultant's audit is a good follow-up to an internal audit. Review and audit your network security at least once a year.

TERM TO KNOW

Security Audit

A thorough examination of your network that includes testing all its components and security controls to make sure everything is secure.

1b. Clean-Desk Policy

Clean-desk policy requires that all important documents, like books, schematics, confidential letters, notes to self, and so on, are not left out in the open when someone is away from their desk. Instead, they must be locked away, securely out of sight. And make sure it is clear that this rule applies to users' PC desktops too. Policies like this apply to offices, laboratories, and workbenches as well as desks, and it is really important for employees who share workspaces or workstations.

TERM TO KNOW

Clean-Desk Policy

A requirement that all important documents like books, schematics, confidential letters, notes to self, etc., are not left out in the open when someone is away from their desk.

1c. Recording Equipment

Recording equipment such as tape recorders, cell phones, and small memory devices, like USB flash memory keychains, can contain sensitive, confidential information, so a good security policy should prohibit their unauthorized presence and use.

1d. Licensing Restrictions

Software piracy is the unauthorized reproduction or distribution of copyrighted software. Security professionals and the organizations they work with must ensure that the organizations take measures to ensure that employees understand the implications of installing pirated software. They also need to ensure that these issues are covered specifically in the security policy.

TERM TO KNOW

Software Piracy

The unauthorized reproduction or distribution of copyrighted software.

1e. Notification

Notify users of the security policies when you give them their usernames and passwords. It is also a good idea to have computers display a summarized version of the policy when any user attempts to connect.

1f. Equipment Access

Disable all unused network ports so that any visitors who happen to be in the building cannot connect a laptop to an unused port and gain access to the network. And be sure to place all network equipment under lock and key.

1g. Wiring

Your network's wires should never run along the floor where they can be easily accessed. Routers, switches, and other network hardware should reside in locked closets or rooms, with access to those rooms controlled by anything ranging from a good lock to a biometric access system, depending on the level of security your specific network and data require.

1h. Door Locks/Swipe Mechanisms

Be sure that only authorized people know the combination to the cipher lock on your data center doors or that only the appropriate people have badges that allow access to the data center. Change lock combinations often, and never ever leave server room doors open or unlocked.

1i. Badges

Require everyone to wear an ID badge, including contractors and visitors, and assign appropriate access levels to everyone. Require badge access to all entrances to buildings and internal computer rooms. Track and record all entry to and exits from these rooms.

1j. Passwords

It has been customary that passwords are set at least every month, however there is some debate about this strategy. Some believe that changing them every 30–45 days weakens the system as users use passwords that are easier to remember, anticipating they will have to change it soon. Train everyone on how to create strong passwords. Set BIOS passwords on every client and server computer to prevent BIOS changes.

1k. Monitor Viewing

Place computer monitors strategically so that visitors or people looking through windows cannot see them, and make sure unauthorized persons cannot see security guard stations and server monitors. Use monitor privacy screens if necessary.

1l. Accounts

Each user should have their own, unique user account, and employees should never share user accounts or passwords. Even temporary employees should have their own account. Otherwise, you may not be able to attribute a security breach to a specific person.

1m. Background Checks

Do background checks on all network support staff. This may include calling their previous employers, verifying their college degrees, requiring drug tests, and checking for criminal background.

1n. Firewalls

Use a firewall to protect all internet connections and use the appropriate proxies and dynamic packet filtering equipment to control access to the network. Your firewall should provide as much security as your company requires and as your budget allows.

1o. Intrusion Detection

Use intrusion detection and logging software to discover security breaches, and be sure you are logging the events you want to monitor.

1p. Cameras

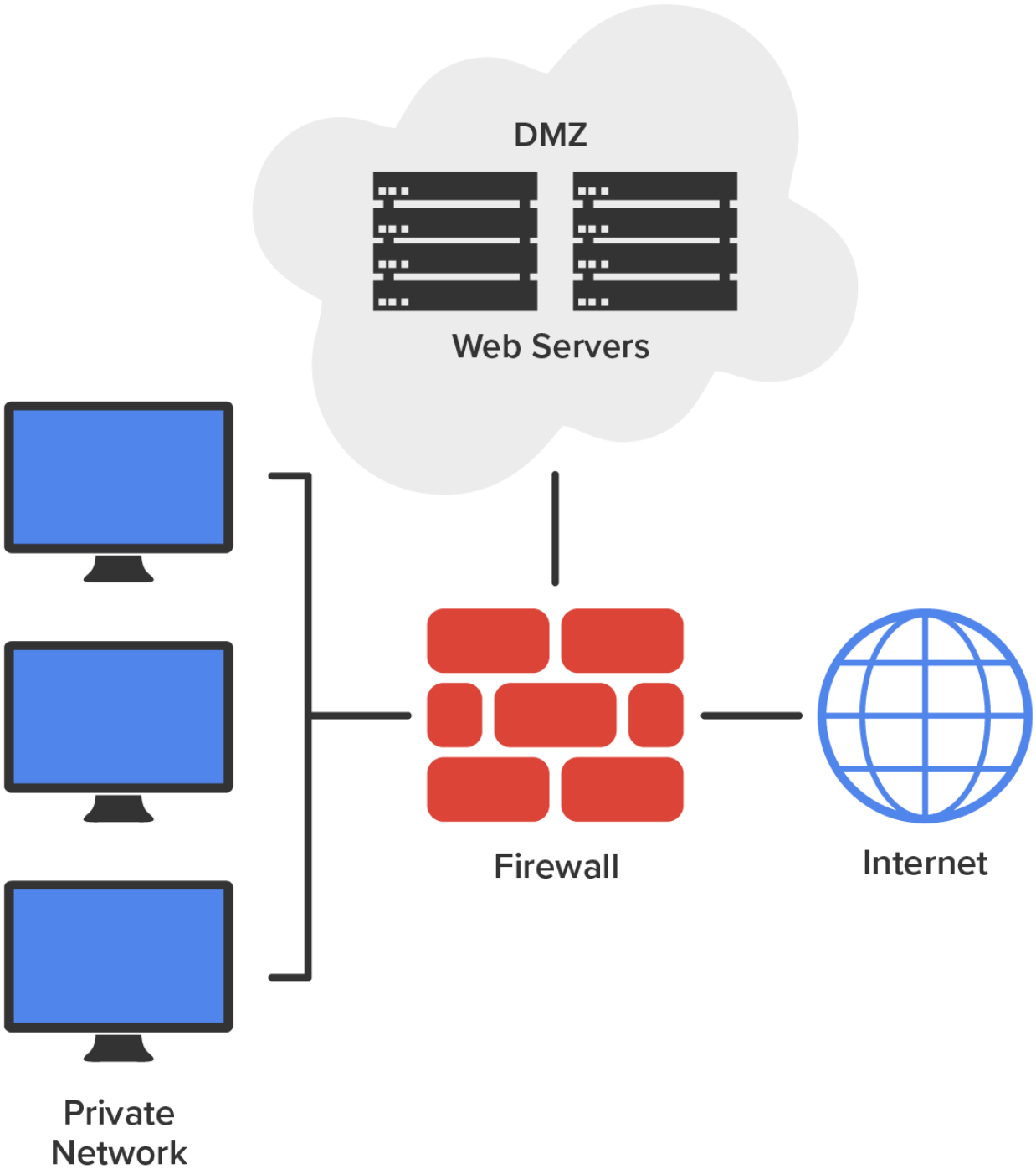
Cameras should cover all entrances to the building and the entire parking lot. Be sure that cameras are in weather-proof and tamper-proof housings, and review the output at a security-monitoring office.

1q. Mail Servers

Provide each person with their own email mailbox, and attach an individual network account to each mailbox. If several people need to access a mailbox, do not give all of them the password to a single network account. Instead, assign individual privileges to each person's network account so you can track activity down to a single person, even with a generic address like info@mycompany.com.

1r. DMZ

Use a demilitarized zone (DMZ) for all publicly viewable servers, including web servers, FTP servers, and email relay servers. The diagram below shows a common DMZ setup.



It is not advisable to put a DMZ outside the firewall because having servers outside your firewall defeats the whole purpose of having one.

1s. Patches

Make sure the latest security updates are installed after being properly tested on a computer that is not connected to the enterprise network.

1t. Backups

Store backup media securely, not on a shelf or table within reach of someone working at the server. Lock backup media in a waterproof, fireproof safe, and keep at least some of your backups off site. Consider using a cloud-based backup service for offsite storage.

1u. Privileged User Accounts

Privileged user accounts represent those that have been provided rights normally reserved for the administrator. For example, if Jeff is granted the right to manage a printer, he now possesses a privileged account. Privileged accounts represent a potential security vulnerability, and their use should be monitored continually to ensure that they are used responsibly. When implementing them, you should always follow the **principle of least privilege**, which specifies that users should only be granted privileges required to do their job.

TERM TO KNOW

Principle of Least Privilege

A principle which specifies that users should only be granted privileges required to do their job.

1v. File Integrity Monitoring

File integrity refers to the prevention of unauthorized data alteration. File hashing can be used to verify that changes to files have not occurred. A **hash function** takes a message of variable length and produces a fixed-length hash value. Hash values, also referred to as message digests, are calculated using the original message. If the receiver calculates a hash value that is the same as the hash value of the original message, the original message is intact. If the receiver calculates a hash value that is different, then the original message has been altered.

TERM TO KNOW

Hash Function

An algorithm that generates a numeric, or fixed-size character output from a variable-sized piece of text or other data.

1w. Role Separation

Separation of duties is a concept that specifies that any operation that is susceptible to fraud or abuse by employees should be broken into two tasks, and these two tasks should be assigned to different individuals. While there is no guarantee that these two individuals will not collude, the chance of that occurring is much less than the chance of a single individual committing fraud.

TERM TO KNOW

Separation of Duties

The requirement that two or more people must be involved in order to complete a high-risk task.

1x. Restricting Access via ACLs

Access control lists identify those who have access to resources and the type of access they have. ACLs are attached to the resource and are consulted whenever an entity requests access. These ACLs are your primary means of preventing access to unauthorized individuals. When implementing them, you should always follow

the principle of least privilege, which specifies that users should only be granted access to information required to do their job.

2. Security Training

This brings us to the human element of network security. It is true that most of your users want to do the right thing to protect the company from a security incident, but the problem is that people do not always know the right thing to do. That is why training is so vital. It can include classroom sessions or web-based training. It is also a good idea to have separate training classes for IT personnel and end users. End-user training may take just an hour or so to keep employees informed. Security training supports the effectiveness of your security policy by helping users know about and understand it. You can even use a year-end bonus or some other incentive as a motivational reward for the employees who complete their training and test well on it.

KEY CONCEPT

It is critical to back up your training program and security policies by providing your end users reference manuals in case they forget something.

EXAMPLE The following are some things to include in reference manuals:

- Recommended policies for creating safe passwords
- The number to call if they've locked themselves out of their accounts
- What to do if they think someone is phishing for information
- What to do if they think their computer has a virus

New employees to the company or division should be required to go through training, but requiring that everybody attend annual refresher courses is also a good idea. And do not hesitate to make an announcement to keep everyone up to date if new threats arise or any sudden changes occur.

2a. Administrator Training

Training sessions for your IT personnel have to be a lot more in depth because they will be the ones who configure and enforce policies, and they will also be the first responders to any security incident.

It is important to cover every aspect of your security policy with these people. And be sure they understand the correct ways to escalate issues in case of an emergency. Reacting to a security incident may be stressful, and you do not want your administrators to panic or feel isolated if one occurs.

2b. Patches and Upgrades

As operating systems and applications are released, their developers have a chance to catch and repair the problems they uncover. In addition, as hackers find and take advantage of vulnerabilities, software developers work to plug those holes as quickly as they can to avoid zero-day exploits. The repairs are usually released to the public as patches or hotfixes.

To address large-scale issues or add major features and components to a program, companies release complete upgrades instead. Here is where we get into the software side of security, which includes things like applying patches, hotfixes, and upgrades. The software aspects of security also include how to choose and install the right third-party software to protect yourself from viruses. Ensuring that your software is up to date is one of the best ways to protect against hackers exploiting the security holes on your network.

SUMMARY

In this lesson, you learned about the importance of **security policies**, which provide a foundation for all network security. Specifically, we addressed several common considerations that should typically be incorporated into an enterprise security policy. Finally, we explored **security training** considerations.

TERMS TO KNOW

Clean-Desk Policy
A requirement that all important documents like books, schematics, confidential letters, notes to self, etc., are not left out in the open when someone is away from their desk.

Hash Function
An algorithm that generates a numeric, or fixed-size character output from a variable-sized piece of text or other data.

Principle of Least Privilege
A principle which specifies that users should only be granted privileges required to do their job.

Security Audit
A thorough examination of your network that includes testing all its components and security controls to make sure everything is secure.

Security Policy
A document that defines what it means to be secure for systems and networks within a particular organization.

Separation of Duties
The requirement that two or more people must be involved in order to complete a high-risk task.

Software Piracy
The unauthorized reproduction or distribution of copyrighted software.