Chapter 16: Advanced Security

IT Essentials: PC Hardware and Software v4.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 16 Objectives

- 16.1 Outline security requirements based on customer needs
- 16.2 Select security components based on customer needs
- 16.3 Implement customer's security policy
- 16.4 Perform preventive maintenance on security
- 16.5 Troubleshoot security

Outline Security Requirements

- An organization should strive to achieve the best and most affordable security protection against data loss or damage to software and equipment.
- A security policy includes a comprehensive statement about the level of security required and how this security will be achieved.
  - Is the computer located at a home or a business?
  - Is there full-time Internet access?
  - Is the computer a laptop?

Outline a Security Policy

- A Security Policy is a collection of rules, guidelines, and checklists:
  - Identify the people permitted to use the computer equipment.
  - Identify devices that are permitted to be installed on a network, as well as the conditions of the installation.
  - Define the requirements necessary for data to remain confidential on a network.
  - Determine a process for employees to acquire access to equipment and data.
  - Define an acceptable computer usage statement.
- The security policy should also provide detailed information about the following issues in case of an emergency:
  - Steps to take after a breach in security
  - Who to contact in an emergency
  - Information to share with customers, vendors, and the media
  - Secondary locations to use in an evacuation
  - Steps to take after an emergency is over, including the priority of services to be restored

Security Hardware

- Identify hardware and equipment that can be used to prevent theft, vandalism, and data loss.
  - To **restrict access** to premises, you might use biometrics, fences, and/or door locks.
  - To **protect the network infrastructure**, you might secure telecom rooms, setup detection for unauthorized use of wireless, and/or setup hardware firewalls.
  - To **protect individual computers**, you might use cable locks, laptop docking station locks and/or lockable cases.
  - To **protect data**, you might use lockable HD carriers and/or USP security dongles.

Security Applications

- Security applications protect the operating system and software application data.
  - Software Firewall
  - Intrusion Detection Systems (IDS)
  - Application and OS Patches
  - Anti-virus software and anti-malware software
- Compare the cost of data loss to the expense of security protection, and then determine what tradeoffs are acceptable.

Selecting Security Components

- Consider the following factors when deciding on security components:

- Advantages and disadvantages of a security component
- Overlapping features and functions
- Component setup and maintenance requirements
- Budget restrictions
- Real and perceived threats

Security Components

- Determine the appropriate techniques to secure equipment and data for the customer.
- Depending on the situation, more than one technique may be required:
  - Passwords
  - Logging and Auditing
  - Wireless Configurations
  - Security Technologies
    - Hash encoding
    - Symmetric encryption
    - Asymmetric encryption
    - VPN

Access Control Devices

- Physical access control devices
  - Lock
  - Conduit
  - Card key
  - Video surveillance
  - Security Guard
- Two-factor identification methods for access control
  - Smart card
  - Security key fob
  - Biometric device

Firewall Types

Hardware Firewall	Software Firewall
• Free-standing and uses dedicated hardware	• Available as 3rd party software and cost varies
• Initial cost for hardware and software updates can be costly	• Included in Windows XP operating system
• Multiple computers can be protected	• Typically protects only the computer it is installed on
• Little impact on the computer performance	• Uses the CPU, potentially slowing the computer

- **Hardware and software firewalls have several modes for filtering network data traffic:**
  - **Packet filtering**
  - **Proxy firewall**
  - **Stateful packet inspection**

Configure Security Settings

- Permissions on folders and files:
  - Use FAT or NTFS to configure folder sharing or folder-level permissions for users with network access
  - Use file-level permissions with NTFS to configure access to files

Permissions	Full Control	Modify	Read and Execute	Read	Write
Execute File	yes	yes	yes	no	no
View Data	yes	yes	yes	yes	no
View File Attributes	yes	yes	yes	yes	no
View Extended Attributes	yes	yes	yes	yes	no
Write Data	yes	yes	no	no	yes
Append Data	yes	yes	no	no	yes
Write File Attributes	yes	yes	no	no	yes
Write Extended File Attributes	yes	yes	no	no	yes
Delete File	yes	yes	no	no	no
View File Permissions	yes	yes	yes	yes	yes
Change File Permissions	yes	no	no	no	no
Take Ownership	yes	no	no	no	no
Synchronize	yes	yes	yes	yes	yes

Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder	yes	yes	yes	yes	no	no
List Folder	yes	yes	yes	yes	yes	no
View Folder Attributes	yes	yes	yes	yes	yes	no
View Extended Folder Attributes	yes	yes	yes	yes	yes	no
Create Files Within the Folder	yes	yes	no	no	no	yes
Create Folders	yes	yes	no	no	no	yes
Write Folder Attributes	yes	yes	no	no	no	yes
Write Extended Folder Attributes	yes	yes	no	no	no	yes
Delete Subfolders and Files	yes	no	no	no	no	no
Delete Folder	yes	yes	no	no	no	no
View Folder Permissions	yes	yes	yes	yes	yes	yes
Change Folder Permissions	yes	no	no	no	no	no
Take Ownership	yes	no	no	no	no	no
Synchronize	yes	yes	yes	yes	yes	yes

Configure Security Settings (Continued)

- Securing wireless access points:
  - Wireless antenna
  - Network Device Access Permissions
  - Service Set Identifier (SSID) Broadcasting
  - MAC address filtering
  - Firewalls
  - Port Forwarding and Port Triggering
  - Wireless Security Modes
    - Wired Equivalent Privacy (WEP)
    - Wi-Fi Protected Access (WPA)
    - Wi-Fi Protected Access 2 (WPA2)
    - Lightweight Extensible Authentication Protocol (LEAP): EAP-Cisco

Configure Firewalls

- A firewall selectively denies traffic to a computer or network segment. Firewalls generally work by opening and closing the ports used by various applications.
- By opening only the required ports on a firewall, you are implementing a restrictive security policy.
- In the past, software and hardware were shipped with permissive settings.
- Software Firewalls can be either an independent application or part of the operating system.

Protect Against Malware

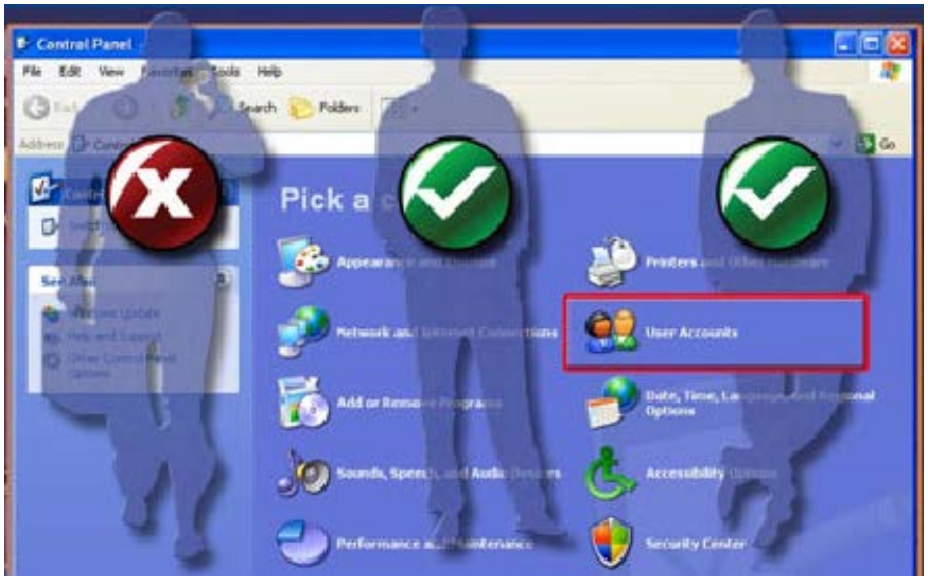
- **Malware** is malicious software that is installed on a computer without the knowledge or permission of the user.
- It may take several different anti-malware programs and multiple scans to completely remove all malicious software.
- Anti-malware available for these purpose are: Anti-virus, anti-spyware, anti-adware, and phishing programs.

Operating System Updates

- Keeping your operating system updated can prevent potential attacks.
- Windows give users the ability to control when software is updated:
  - **Automatic**: Automatically downloads and installs without user intervention.
  - **Only Download Updates**: Download the updates automatically, but the user is required to install them.
  - **Notify Me**: Notify the user that updates are available and gives the user the option to download and install.
  - **Turn off Automatic Updates**: Prevents automatically checking for updates. Updates have to be discovered, downloaded and installed by the user.

User Account Maintenance

- Group employees by job requirements to give access to files by setting up group permissions.
- When an employee leaves an organization, access to the network should be terminated immediately.
- Guests can be given access through a Guest account.



Data Backups

- A data backup stores a copy of the information on a computer to removable backup media that can be kept in a safe place. If the computer hardware fails, the data backup can be restored so that processing can continue.
- Data backups should be performed on a regular basis.

	Description
Full or Normal Backup	Archives all selected files.
Incremental Backup	Archives all selected files that have changed since last full or incremental backup. It marks files as having been backed up.
Differential Backup	Archives everything that has changed since last full backup. It does not mark files as having been backed up.
Daily Backup	Archives all selected files that have changed on the day of the backup.
Copy Backup	Archives all selected files.

Troubleshooting Process

Step 1 Identify the problem

Step 2 Establish a theory of probable causes

Step 3 Determine an exact cause

Step 4 Implement a solution

Step 5 Verify solution and full system functionality

Step 6 Document findings

Step 1 - Identify the Problem

- **Hardware/Software information**
  - Manufacturer, model, OS, network environment, connection type
- **Open-ended questions**
  - What problems are you experiencing?
  - When did the problem start?
  - How are you connected to the Internet?
  - What type of firewall are you using?
  - What security software is installed on your computer?
  - What resource permissions do you have?
- **Closed-ended questions**
  - Do you have a firewall?
  - Has anyone else used your computer?
  - Is your security software up to date?
  - Have you scanned your computer recently for viruses?
  - Have you ever had this problem before?
  - Have you changed your password recently?
  - Have you received any error messages on your computer?
  - Have you shared your password?
  - Do you have permissions for the resource?

Step 2 - Establish a Theory of Probable Causes

- Problem may be simpler than the customer thinks.

- Create a list of the most common reasons why the error would occur:
  - The user account is disabled.
  - The user is using an incorrect username or password.
  - The user does not have the correct folder or file permissions.
  - The user's computer has been infected by a virus.
  - The wireless security configurations are incorrect on the client.
  - The security configurations are incorrect on the wireless access point.

Step 3 - Determine the Exact Cause

- Testing your theories of probable causes one at a time, starting with the quickest and easiest.
  - Verify the user's account settings.
  - Reset the user's password.
  - Verify the user's permissions for folders and files.
  - Check firewall logs for errors.
  - Verify the firewall settings.
  - Scan and remove viruses from the computer.
  - Verify the wireless security configuration of the client.
  - Verify the security configuration on the wireless access point.
- If the exact cause of the problem has not been determined after you have tested all your theories, establish a new theory of probable causes and test it.

Step 4 - Implement a Solution

- Sometimes quick procedures can determine the exact cause of the problem or even correct the problem.
- If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.
- Divide larger problems into smaller problems that can be analyzed and solved individually.

Step 5 - Verify Solution and System Functionality

- Verifying full system functionality and implementing any preventive measures if needed. Ensures that you have not created another problem while repairing the computer.
  - Reboot the computer.
  - Log on the computer.
  - Connect to the network using wireless.
  - Verify file and folder access.
  - Verify that no virus is found with a virus scan.

- Have the customer verify the solution and system functionality.

Step 6 - Document Findings

- Discuss the solution with the customer
- Have the customer confirm that the problem has been solved
- Document the process
  - Problem description
  - Solution
  - Components used
  - Amount of time spent in solving the problem

Common Problems and Solutions

- Network problems can be attributed to hardware, software, networks, or some combination of the three. You will resolve some types of problems more often than others, while other problems may require more in-depth troubleshooting skills.

Apply Troubleshooting Skills

- It is time to apply your listening and diagnostic skills.

Chapter 16 Summary

- Security threats can come from inside or outside of an organization.
- Viruses and worms are common threats that attack data.
- Develop and maintain a security plan to protect both data and physical equipment from loss.
- Keep operating systems and applications up to date and secure with patches and service packs.