Chapter 9: Fundamental Security

IT Essentials: PC Hardware and Software v4.1

Cisco | Networking Academy®
Mind Wide Open™

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Chapter 9 Objectives

- 9.1 Explain why security is important
- 9.2 Describe security threats
- 9.3 Identify security procedures
- 9.4 Identify common preventive maintenance techniques for security
- 9.5 Troubleshoot security

© 2007-2010 Cisco Systems, Inc. All rights reserved.

The Importance of Security

- Private information, company secrets, financial data, computer equipment, and items of national security are placed at risk if proper security procedures are not followed.
- A technician's primary responsibilities include data and network security.

© 2007-2010 Cisco Systems, Inc. All rights reserved.
Cisco Public

Security Threats

Types of attacks to computer security:

- Physical
  - Theft, damage, or destruction to computer equipment.
- Data
  - Removal, corruption, denial of access, unauthorized access, or theft of information.

Potential threats to computer security:

- Internal threats
  - Employees can cause a malicious threat or an accidental threat.
- External threats
  - Outside users can attack in an unstructured or structured way.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

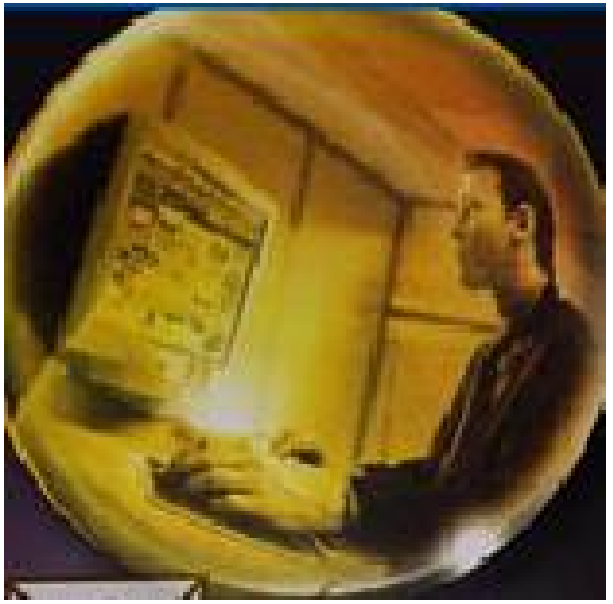
Viruses, Worms, and Trojan Horses

- Malicious software (malware) is any software designed to damage or to disrupt a system:
  - **Virus** is a software code that is deliberately created by an attacker. Viruses may collect sensitive information or may alter or destroy information.
  - A **worm** is a self-replicating program that uses the network to duplicate its code to the hosts on the network. At a minimum, worms consume bandwidth in a network.
  - A **Trojan horse** is technically a worm and is named for its method of getting past computer defenses by pretending to be something useful.
- Anti-virus software is designed to detect, disable, and remove viruses, worms, and Trojan horses before they infect a computer.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Web Security

Attackers may use any of these tools to install a program on a computer.



- ActiveX
  - Controls interactivity on web pages
- Java
  - Allows applets to run within a browser
  - Example: a calculator or a counter
- JavaScript
  - Interacts with HTML source code to allow interactive web sites
  - Example: a rotating banner or a popup window

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Adware, Spyware, and Grayware

- Typically installed without the user's knowledge, these programs collect information stored on the computer, change the computer configuration, or open extra windows on the computer and all without the user's consent.
  - **Adware** displays advertising, usually in a popup window.
  - **Grayware** or malware is a file or program other than a virus that is potentially harmful.
  - **Spyware**, a type of grayware, is distributed without any user intervention of knowledge.
  - **Phishing** is a form of social engineering where the attacker pretends to represent a legitimate outside organization.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Denial of Service (DoS)

- Prevents users from accessing normal services
- Sends enough requests to overload a resource or even stopping its operation
  - **Ping of Death** is a series of repeated, larger than normal pings intended to crash the receiving computer
  - **E-mail Bomb** is a large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing e-mail
  - **Distributed DoS** is an attack launched from many computers, called **zombies**

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Spam and Popup Windows

- **Spam** is unsolicited email that can be used to send harmful links or deceptive content.
- **Popups** are windows that automatically open and are designed to capture your attention and lead you to advertising sites.

Use anti-virus software, options in e-mail software, popup blockers, and common indications of spam to combat these.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Social Engineering

- A social engineer is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information.
  - Never give out a password
  - Always ask for the ID of the unknown person
  - Restrict access of unexpected visitors
  - Escort all visitors through the facility

© 2007-2010 Cisco Systems, Inc. All rights reserved.

TCP/IP Attacks

- TCP/IP is used to control all Internet communications.

© 2007-2010 Cisco Systems, Inc. All rights reserved.
Cisco Public

Computer Disposal and Recycling

- Erase all hard drives, then use a third-party tool to fully erase all data.
- The only way to fully ensure that data cannot be recovered from a hard drive is to carefully shatter the platters with a hammer and safely dispose of the pieces.
- To destroy software media (floppy disks and CDs), use a shredding machine designed for shredding these materials.
- Three methods are commonly used to either destroy or recycle data and hard drives:
  - Data wiping
  - Hard drive destruction
  - Hard drive recycling

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

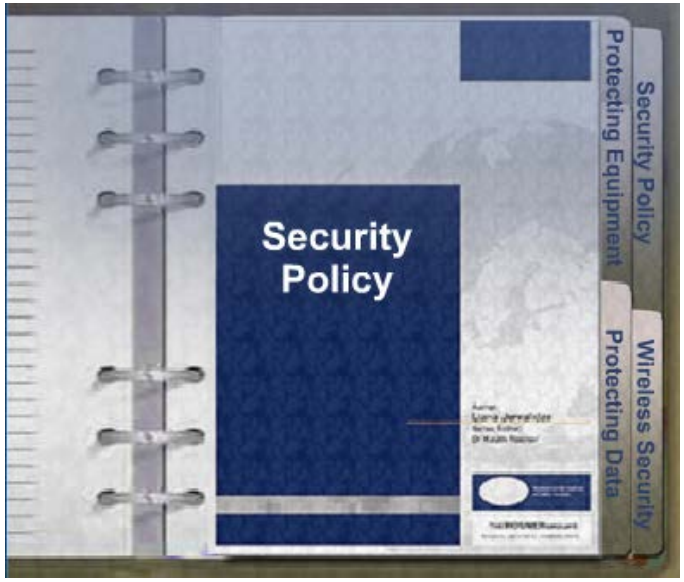
Security is Strengthened in Layers

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Security Policy

- A security policy should describe how a company addresses security issues, as shown in Figure 1.

- Questions to answer in writing a local security policy:
  - What assets require protection?
  - What are the possible threats?
  - What should be done in the event of a security breach?



© 2007-2010 Cisco Systems, Inc. All rights reserved.
Cisco Public

Protecting Equipment

- Since stealing the whole PC is the easiest way to steal data, physical computer equipment must be secured.
- Some methods of physically protecting computer equipment are:
  - Control access to facilities
  - Use cable locks with equipment
  - Keep telecommunication rooms locked
  - Fit equipment with security screws
- Some means to protecting access to facilities are:
  - Card keys are identity cards with a chip that stores user data, including the level of access
  - Berg connectors for connecting to a floppy drive
  - Biometric sensors that identify physical characteristics of the user, such as a fingerprint or retina

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Protecting Data

- The value of physical equipment is often far less than the value of the data it contains. To protect data, there are several methods of security protection that can be implemented.
  - Password protection
  - Data encryption
  - Software Firewall
  - Data backups
  - Smartcard Security
  - Biometric Security
  - File system security

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Wireless Security Techniques

- Modify the default SSID.
- Set up separate WLAN (SSID/VLAN).
- Use strong encryption.
- Deploy mutual authentication between the client and the network.
- Use VPNs or Wired Equivalent Privacy (WEP) combined with MAC address filters to secure business-specific devices that do not support WPA or WPA2.
- Deploy a lightweight access point architecture that does not store security information locally.
- Ensure management ports are secured.
- Physically hide or secure access points to prevent tampering.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Installing Updates and Patches

- Regular security updates are essential in order to meet the threat from attackers constantly searching for new ways of breaching security.
- A technician should understand how to install patches and updates. They should also be able to recognize when new updates and patches are available.

© 2007-2010 Cisco Systems, Inc. All rights reserved.

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

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Step 1 - Identify the Problem

- System Information
  - Manufacturer, model, OS, network environment, connection type
- Open-ended questions
  - When did the problem start?
  - What problems are you experiencing?
  - What websites have you visited recently?
  - What security software is installed in your computer?
  - Who else has used your computer recently?
- Closed-ended questions
  - Is your security software up to date?
  - Have you scanned your computer recently for viruses?
  - Did you open any attachments from a suspicious e-mail?
  - Have you changed your password recently?
  - Have you shared your password?

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

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.
  - Virus
  - Trojan Horse
  - Worm
  - Spyware
  - Adware
  - Grayware or Malware
  - Phishing scheme
  - Password compromised
  - Unprotected equipment rooms
  - Unsecured work environment

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Step 3 - Determine the Exact Cause

- Test your theories of probable causes one at a time, starting with the quickest and easiest.
  - Disconnect from the network
  - Update anti-virus and spyware signatures
  - Scan computer with protection software
  - Check computer for the latest OS patches and updates
  - Reboot the computer or network device
  - Login as a different user to change your password
  - Secure equipment rooms
  - Secure work environment
  - Enforce security policy

- 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.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

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.

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Step 5 - Verify Solution and System Functionality

- Verifying full system functionality and implementing any preventive measures if needed.
  - Re-scan computer to ensure no viruses remain.
  - Re-scan computer to ensure no spyware remains.
  - Check the security software logs to ensure no problems remain.
  - Test network and Internet connectivity.
  - Ensure all application are working.
  - Verify access to authorized resources such as shared printer and databases..
  - Make sure entries are secured.
  - Ensure security policy is enforced.
- Have the customer verify the solution and system functionality.

© 2007-2010 Cisco Systems, Inc. All rights reserved.

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

© 2007-2010 Cisco Systems, Inc. All rights reserved.
Cisco Public

Common Problems and Solutions

- Laptop problems can be attributed to hardware, software, networks, or some combination of the three. You will resolve some types of laptop problems more often than others.

© 2007-2010 Cisco Systems, Inc. All rights reserved.

Chapter 9 Summary

- Following proper security procedures will protect computers and network equipment, and the data they contain, from physical danger such as fire and theft, as well as from loss and damage by employees and attackers.
- 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.

© 2007-2010 Cisco Systems, Inc. All rights reserved. Cisco Public

© 2007-2010 Cisco Systems, Inc. All rights reserved.