Topic 4: Basic Network Security

Technicians need to understand computer and network security. Failure to implement proper security procedures can have an impact on users, computers, and the general public. Private information, company secrets, financial data, computer equipment, and items of national security are placed at risk if proper security procedures are not followed.

Importance of Network Security

Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.
An attack that intentionally degrades the performance of a computer or network can also harm the production of an organization. Poorly implemented security measures to wireless network devices demonstrate that physical connectivity is not necessary for unauthorized access by intruders.

The primary responsibilities of a technician include data and network security. A customer or an organization may depend on you to ensure that their data and computer equipment are secure. You will perform tasks that are more sensitive than those assigned to the average employee. You may repair, adjust, and install equipment. You will need to know how to configure settings to keep the network secure but still keep it available to those who need to access it. You will ensure that software patches and updates are applied, anti-virus software is installed, and anti-spyware software is used. You may also be asked to instruct users how to maintain good security practices with computer equipment.

Security Threats

To successfully protect computers and the network, a technician must understand both types of threats to computer security:

- Physical – Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring
- Data – Events or attacks that remove, corrupt, deny access, allow access, or steal information

Threats to security can come from the inside or outside of an organization, and the level of potential damage can vary greatly:

- Internal – Employees have access to data, equipment, and the network
- Malicious threats are when an employee intends to cause damage.
- Accidental threats are when the user damages data or equipment unintentionally.
- External – Users outside of an organization that do not have authorized access to the network or resources
- Unstructured – Attackers use available resources, such as passwords or scripts, to gain access and run programs designed to vandalize
- Structured – Attackers use code to access operating systems and software

Physical loss or damage to equipment can be expensive, and data loss can be detrimental to your business and reputation. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

Virus, Worms, and Trojans.

Computer viruses are deliberately created and sent out by attackers. A virus is attached to small pieces of computer code, software, or documents. The virus executes when the software is run on a computer. If the virus is spread to other computers, those computers could continue to spread the virus.

A **virus** is a program written with malicious intent and sent out by attackers. The virus is transferred to another computer through e-mail, file transfers, and instant messaging. The virus hides by attaching itself to a file on the computer. When the file is accessed, the virus executes and infects the computer. A virus has the potential to corrupt or even delete files on your computer, use your e-mail to spread itself to other computers, or even erase your entire hard drive.

Some viruses can be exceptionally dangerous. The most damaging type of virus is used to record keystrokes. These viruses can be used by attackers to harvest sensitive information, such as passwords and credit card numbers. Viruses may even alter or destroy information on a computer. Stealth viruses can infect a computer and lay dormant until summoned by the attacker.

A **worm** is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Even if the worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth.

A **Trojan** is technically a worm. The Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another. Trojans are often disguised as useful software. The Trojan program can reproduce like a virus and spread to other computers. Computer data damage and production loss could be significant. A technician may be needed to perform the repairs, and employees may lose or have to replace data. An infected computer could be sending critical data to competitors, while at the same time infecting other computers on the network.

Virus protection software, known as anti-virus software, is software designed specifically to detect, disable, and remove viruses, worms, and Trojans before they infect a computer. Anti-virus software becomes outdated quickly, however, and it is the responsibility of the technician to apply the most recent updates, patches, and virus definitions as part of a regular maintenance schedule. Many organizations establish a written security policy stating that employees are not permitted to install any software that is not provided by the company. Organizations also make employees aware of the dangers of opening e-mail attachments that may contain a virus or a worm.

Web Security

Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.

Tools that are used to make web pages more powerful and versatile can also make computers more vulnerable to attacks. These are some examples of web tools:

- ActiveX – Technology created by Microsoft to control interactivity on web pages. If ActiveX is on a page, an applet or small program has to be downloaded to gain access to the full functionality.

- Java – Programming language that allows applets to run within a web browser. Examples of applets include a calculator or a counter.
- JavaScript – Programming language developed to interact with HTML source code to allow interactive websites. Examples include a rotating banner or a popup window.

Attackers may use any of these tools to install a program on a computer. To prevent against these attacks, most browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript.

Adware, Spyware, and Grayware

Adware, spyware, and grayware are usually installed on a computer without the knowledge of the user. These programs collect information stored on the computer, change the computer configuration, or open extra windows on the computer without the user's consent.

Adware is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them.

Grayware or malware is a file or program other then a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Grayware can be removed using spyware and adware removal tools.

Spyware, a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

Phishing is a form of social engineering where the attacker pretends to represent a legitimate outside organization, such as a bank. A potential victim is contacted via e-mail. The attacker might ask for verification of information, such as a password or username, to supposedly prevent some terrible consequence from occurring.

Denial of Service

Denial of service (DoS) is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

Common DoS attacks include the following:

1. Ping of death – A series of repeated, larger than normal pings that crash the receiving computer
2. E-mail bomb – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

Distributed DoS (DDoS) is another form of attack that uses many infected computers, called zombies, to launch an attack. With DDoS, the intent is to obstruct or overwhelm access to the targeted server. Zombie computers located at different geographical locations make it difficult to trace the origin of the attack.

Spam and Popup Windows

Spam, also known as junk mail, is unsolicited e-mail. In most cases, spam is used as a method of advertising. However, spam can be used to send harmful links or deceptive content.

When used as an attack method, spam may include links to an infected website or an attachment that could infect a computer. These links or attachments may result in lots of windows designed to capture your attention and lead you to advertising sites. These windows are called popups. Uncontrolled popup windows can quickly cover the user's screen and prevent any work from getting done.

Many anti-virus and e-mail software programs automatically detect and remove spam from an e-mail inbox. Some spam still may get through, so look for some of the more common indications:

- No subject line
- Incomplete return addresses
- Computer generated e-mails
- Return e-mails not sent by the user

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. Often, the social engineer gains the confidence of an employee and convinces the employee to divulge username and password information.

A social engineer may pose as a technician to try to gain entry into a facility. Once inside, the social engineer may look over shoulders to gather information, seek out papers on desks with passwords and phone extensions, or obtain a company directory with e-mail addresses.
Here are some basic precautions to help protect against social engineering:

- Never give out your password
- Always ask for the ID of unknown persons
- Restrict access of unexpected visitors
- Escort all visitors
- Never post your password in your work area
- Lock your computer when you leave your desk
- Do not let anyone follow you through a door that requires an access card

TCI/IP Attacks

TCP/IP is the protocol suite that is used to control all of the communications on the Internet. Unfortunately, TCP/IP can also make a network vulnerable to attackers.
Some of the most common attacks:

- SYN Flood – Randomly opens TCP ports, tying up the network equipment or computer with a large amount of false requests, causing sessions to be denied to others
- DoS – Sends abnormally large amounts of requests to a system preventing access to the services
- DDoS – Uses "zombies" to make tracing the origin of the DoS attack difficult to locate
- Spoofing – Gains access to resources on devices by pretending to be a trusted computer
- Man-in-the-Middle – Intercepts or inserts false information in traffic between two hosts
- Replay – Uses network sniffers to extract usernames and passwords to be used at a later date to gain access
- DNS Poisoning – Changes the DNS records on a system to point to false servers where the data is recorded

Hardware Deconstruction and Recycling

Hardware deconstruction is the process of removing sensitive data from hardware and software before recycling or discarding. Hard drives should be fully erased to prevent the possibility of recovery using specialized software. It is not enough to delete files or even format the drive. Use a third party tool to overwrite data multiple times rendering the data unusable. 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.

Media like CDs and floppy disks must also be destroyed. Use a shredding machine that is designed for the purpose.

Security Procedures

A security plan should be used to determine what will be done in a critical situation. Security plan policies should be constantly updated to reflect the latest threats to a network. A security plan with clear security procedures is the basis for a technician to follow. Security plans should be reviewed on a yearly basis.

Part of the process of ensuring security is to conduct tests to determine areas where security is weak. Testing should be done on a regular basis. New threats are released daily. Regular testing provides details of any possible weaknesses in the current security plan that should be addressed.

There are multiple layers of security in a network, including physical, wireless, and data. Each layer is subject to security attacks. The technician needs to understand how to implement security procedures to protect equipment and data.

Basic Local Security Policy Requirements

Though local security policies may vary between organizations, there are questions all organizations should ask:

- What assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?
- NOTE: The computer itself may be referred to as the central processing unit, or CPU. For this course, the term CPU will only refer to the microprocessor chip.
- A security policy should describe how a company addresses security issues:
- Define a process for handling network security incidents
- Define a process to audit existing network security
- Define a general security framework for implementing network security
- Define behaviors that are allowed
- Define behaviors that are prohibited
- Describe what to log and how to store the logs: Event Viewer, system log files, or security log files
- Define network access to resources through account permissions
- Define authentication technologies to access data: usernames, passwords, biometrics, smart cards

Tasks Required to Protect Physical Equipment

Physical security is as important as data security. When a computer is taken, the data is also stolen.

There are several methods of physically protecting computer equipment.

- Control access to facilities
- Use cable locks with equipment
- Keep telecommunication rooms locked
- Fit equipment with security screws
- Use security cages around equipment
- Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment

For access to facilities, there are several means of protection:

- Card keys that store user data, including level of access
- Berg connecters for connecting to a floppy drive
- Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
- Posted security guard
- Sensors, such as RFID tags, to monitor equipment
- Ways to Protect Data

The value of physical equipment is often far less than the value of the data it contains. The loss of sensitive data to a company's competitors or to criminals may be costly. Such losses may result in a lack of confidence in the company and the dismissal of computer technicians in charge of computer security. To protect data, there are several methods of security protection that can be implemented.

Password Protection

Password protection can prevent unauthorized access to content. Attackers are able to gain access to unprotected computer data. All computers should be password protected. Two levels of password protection are recommended:

- BIOS – Prevents BIOS settings from being changed without the appropriate password
- Login – Prevents unauthorized access to the network

Network logins provide a means of logging activity on the network and either preventing or allowing access to resources. This makes it possible to determine what resources are being accessed. Usually, the system administrator defines a naming convention for the usernames when creating network logins. A common example of a username is the first initial of the person's first name and then the entire last name. You should keep the username naming convention simple so that people do not have a hard time remembering it.

When assigning passwords, the level of password control should match the level of protection required. A good security policy should be strictly enforced and include, but not be limited to, the following rules:

- Passwords should expire after a specific period of time.
- Passwords should contain a mixture of letters and numbers so that they cannot easily be broken.

Password standards should prevent users from writing down passwords and leaving them unprotected from public view.

Rules about password expiration and lockout should be defined. Lockout rules apply when an unsuccessful attempt has been made to access the system or when a specific change has been detected in the system configuration.

To simplify the process of administrating security, it is common to assign users to groups, and then to assign groups to resources. This allows the access capability of users on a network to be changed easily by assigning or removing the user from various groups. This is useful when setting up temporary accounts for visiting workers or consultants, giving you the ability to limit access to resources.

Data Encryption

Encrypting data uses codes and ciphers. Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption. It may not be possible to decipher captured data in time to make any use of it.

Virtual Private Network (VPN) uses encryption to protect data. A VPN connection allows a remote user to safely access resources as if their computer is physically attached to the local network.

Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A firewall is a way of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is called traffic.

DataBackups

Data backup procedures should be included in a security plan. Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood. Backing up data is one of the most effective ways of protecting against data loss. Here are some considerations for data backups:

- Frequency of backups – Backups can take a long time. Sometimes it is easier to make a full backup monthly or weekly, and then do frequent partial backups of any data that has changed since the last full backup. However, spreading the backups over many recordings increases the amount of time needed to restore the data.
- Storage of backups – Backups should be transported to an approved offsite storage location for extra security. The current backup media is transported to the offsite location on a daily, weekly, or monthly rotation as required by the local organization.
- Security of backups – Backups can be protected with passwords. These passwords would have to be entered before the data on the backup media could be restored.

File System Security

All file systems keep track of resources, but only file systems with journals can log access by user, date, and time. The FAT 32 file system which is used in some versions of Windows, lacks both journaling and encryption capabilities. As a result, situations that require good security are usually deployed using a file system such as NTFS, which is part of Windows 2000 and Windows XP. If increased security is needed, it is possible to run certain utilities, such as CONVERT, to upgrade a FAT 32 file system to NTFS. The conversion process is not reversible. It is important to clearly define your goals before making the transition.

Wireless Security Techniques

Since traffic flows through radio waves in wireless networks, it is easy for attackers to monitor and attack data without having to physically connect to a network. Attackers gain access to a network by being within range of an unprotected wireless network. A technician needs to know how to configure access points and wireless network interface cards (NICs) to an appropriate level of security.

When installing wireless services, you should apply wireless security techniques immediately to prevent unwanted access to the network. Wireless access points should be configured with basic security settings that are compatible with the existing network security.
An attacker can access data as it travels over the radio signal. A wireless encryption system can be used to prevent unwanted capture and use of data by encoding the information that is sent. Both ends of every link must use the same encryption standard. The levels of security described here:

- Wired Equivalent Privacy (WEP) – the first generation security standard for wireless. Attackers quickly discovered that WEP encryption was easy to break. The encryption keys used to encode the messages could be detected by monitoring programs. Once the keys were obtained, messages could be easily decoded.

- Wi-Fi Protected Access (WPA) – an improved version of WEP. It was created as a temporary solution until the 802.11i (a security layer for wireless systems) was fully implemented. Now that 802.11i has been ratified, WPA2 has been released. It covers the entire 802.11i standard.
- Lightweight Extensible Authentication Protocol (LEAP), also called EAP-Cisco – a wireless security protocol created by Cisco to address the weaknesses in WEP and WPA. LEAP is a good choice when using Cisco equipment in conjunction with operating systems like Windows and Linux.
- Wireless Transport Layer Security (WTLS) is a security layer used in mobile devices that employ the Wireless Applications Protocol (WAP). Mobile devices do not have a great deal of spare bandwidth to devote to security protocols. WTLS was designed to provide security for WAP devices in a bandwidth-efficient manner.

Preventive Maintenance Techniques for Security

Security is a constantly changing process and technology. New exploits are discovered daily. Attackers are constantly searching for new methods to use in an attack. Software manufacturers have to regularly create and issue new patches to fix flaws and vulnerabilities in products. If a computer is left unprotected by a technician, an attacker can easily gain access. Unprotected computers on the Internet may become infected within a few minutes.

Because of the constantly changing security threats, a technician should understand how to install patches and updates. They should also be able to recognize when new updates and patches are available. Some manufacturers release updates on the same day every month, but also send out critical updates when necessary. Other manufacturers provide automatic update services that patch the software every time the computer is turned on, or e-mail notifications when a new patch or update is released.

Updating Signature Files for Anti-virus and Anti-Spyware Software

Threats to security from viruses and worms are always present. Attackers constantly look for new ways to infiltrate computers and networks. Because new viruses are always being developed, security software must be continually updated. This process can be performed automatically, but a technician should know how to manually update any type of protection software and all customer application programs.

Virus, spyware, and adware detection programs look for patterns in the programming code of the software in a computer. These patterns are determined by analyzing viruses that are intercepted on the Internet and on LANs. These code patterns are called signatures. The publishers of protection software compile the signatures into virus definition tables. To update signature files for anti-virus and spyware software, first check to see if the signature files are the most recent files. This can be done by navigating to the "About" option of the protection software, or by launching the update tool for the protection software. If the signature files are out of date, update them manually with the "Update Now" option on most protection software. You should always retrieve the signature files from the manufacturer’s website to make sure the update is authentic and not corrupted by viruses. This can put great demand on the manufacturer's website especially when new viruses are released. To avoid creating too much traffic at a single website, some manufacturers distribute their signature files for download to multiple download sites. These download sites are called mirrors.

CAUTION: When downloading the signature files from a mirror, ensure that the mirror site is a legitimate site. Always link to the mirror site from the manufacturer's website.

Installing OS Service Packs and Security Patches

Viruses and worms can be difficult to remove from a computer. Software tools are required to remove viruses and repair the computer code the virus has modified. These software tools are provided by operating system manufacturers and security software companies. Make sure that you download these tools from a legitimate site.

Manufacturers of operating systems and software applications may provide code updates called patches that prevent a newly discovered virus or worm from making a successful attack. From time to time, manufacturers combine patches and upgrades into a comprehensive update application called a service pack. Many infamous and devastating virus attacks could have been much less severe if more users had downloaded and installed the latest service pack.

The Windows operating system routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threat. These updates can include security updates, critical updates, and service packs. Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs, or notifies you as these updates become available.

Updates must be installed, not just downloaded. If you use the Automatic setting you can schedule the time and day. Otherwise, new updates are installed at 3 A.M. by default. If your computer is turned off during a scheduled update, updates are installed the next time you start your computer. You can also choose to have Windows notify you when a new update is available and install the update yourself.

Adapted and Compiled from:

CCNA IT Essential, “PC Hardware and Software” version 4.0, Cisco Networking Academy
CCNA Discovery 1, “Networking for Home and Small Businesses”, Cisco Networking Academy
CCNA Discovery 2, “Working at a Small-to-Medium Business of ISP”, Cisco Networking Academy
CCNA Exploration 1, “Network Fundamentals”, Cisco Networking Academy
Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide, Cisco Press