Security 1623

Assessor name: THAI MINH TUAN

Student Name: PHAM CAO NGUYEN

Student ID: GCC18074

Class: GCC0803

P1 Identify types of security threat to organisations.

- Introduction
  - Brief introduction to Security
- Digital Security Risks:
  - MALWARE.
- Circulation/Infection.
  - Viruses.

    A virus is a malicious type that can copy itself to other computers and propagate. When a user begins one of those contaminated applications, viruses propagate to other machines by linking themselves to different programs and using javascript. Viruses can also distribute bugs in web applications by way of script archives, attachments, and cross-site scripting. Viruses can be used for stolen information, malicious machines and networks, botnets and stealing of capital, notoriety making, etc.

  - Worms.

    The most every kinds of ransomware are machine worms. By using operating system bugs, they propagate across computer networks. Worms normally harm their host networks by bandwidth consumption and web servers overload. Computer worms can also contain payloads to host computers that damage them.

  - Trojan horses.
    - Common strategies:
    - Defend against Trojan horses with the following products:

- Rootkit.

Rootkit is a malicious program that installs and executes malicious code on a system without user consent in order to gain administrator-level access to a computer or network system. There are different types of Rootkit virus such as Bootkits, Firmware Rootkits, Kernel-Level Rootkits, and application Rootkits

- Collect data.
  - Spyware.

Spyware is a form of malware that works by spying on user behavior without its knowledge. The spying techniques could include monitoring behavior, review of keystrokes, a compilation of data (account records, logins, financial information), and more. Additional functions, from modifying software or device security parameters to communicating with network connections, are often frequently used in Spyware. Spyware spreads through the use of software vulnerabilities, the combination of legitimate programs or Trojan software.

  - Adware.

In a way that is unexpected and unwanted by the user, Adware delivers advertising content. When the adware malware becomes installed, it usually shows advertisement banners, popup advertisements, or opens new web browser windows at irregular intervals. Adware is a type of malware that delivers notoriety automatically (Short for advertising-supported software). Pop-up advertisements on software-displayed websites and advertisements are typical examples of adware. “free” versions packaged with adware are often sold by apps and applications.

  - Ransomware

Ransomware prevents a user’s device from properly operating until a fee is paid. One type of ransomware locks up the machine of a victim and then shows a message from a law enforcement agency that purports to arrive.

  - Careless employees
  - Natural disaster.
  - Delete data
  - Modify system Security
    - Back doors
- Networking-Based Attacks

- Denial of Service (DoS)
  - A DoS attack is a deliberate attempt to prevent authorized users from accessing a system by overwhelming that system with requests.
  - Most DoS attacks today are actually distributed denial of service (DDoS) attacks: instead of using one computer, a DDoS may use hundreds or thousands of zombie computers in a botnet to flood a device with requests.
- Types of DoS attacks

A large number of ICMP echo requests are submitted rapidly by several machines, flooding a server (as well as the network) to the point that it will not respond enough quickly and will lose valid connections to other clients and deny all new connections.

- Smurf attack
  - An intruder broadcasts a ping message to all network machines but switches the address from which the request came to the computer of the victim.
  - Each computer then sends a reaction to the computer of the victim such that it is overloaded quickly and then fails or becomes useless to legal users.
- SYN Flood attack
  - Poisoning
  - Attacks on Access Rights

- Application Attacks.
  - Introduction
  - Server-Side Web Application Attacks
    - On the Internet, utilities that are introduced as online apps are delivered by a web server.
    - An significant aspect of web apps on the server-side is that they generate interactive content based on user inputs.
    - Many web application server-side attacks target the feedback that users embrace from the applications.
  - SQL injection:
  - XML Injection:

- Cross-site scripting:
  - Client-side Application Attacks.
  - Header Manipulation.
  - Cookies
  - Attachments
  - Session Hijacking
  - Malicious Add-ons
  - Impartial Overflow Attacks.
  - Social Engineering Attacks
  - Social Engineering
  - Password Guessing
  - TCP/IP Hijacking

- Directory Traversal/Command Injection

- Networking-Based Attacks:
  - Introduction

    Network security attacks constitute illegal activity for the loss, alteration, or stealing of sensitive data against an individual, business, or government IT infrastructure. As more businesses allow workers to view mobile devices' info, networks become prone to computer extortion or full data or network loss. Network-based attacks are dangers that machines or devices other than the ones under attack initiate and handle.

  - Denial of Service (DoS).
    - Buffer overflow:
    - Smurf attack:
    - SMY flood:
  - Interception:
    - Man-in-the-Middle attack:
    - Replay attack:
  - Poisoning

- ARP Poisoning:

- Attacks on Access Rights
- Natural Impact:
- Human impact:

P2 Describe organizational security procedures.

- What is a security procedure?
- Acceptable Use Policy (AUP).
- Access Control Policy (ACP).
- Change Management Policy.
- Information Security Policy.
- Incident Response (IR) Policy.
- Remote Access Policy.
- Email/Communication Policy.
- Disaster Recovery Policy
- Assessing network security risks

- Boost employee knowledge of data protection
- Data security administration
- Fix and manage incidents
- Safely customize the scheme
- Ensuring that the network is broken into different areas
- Stable corporate data by network security management
- Access control
- Increased security from malware
- Updating the patches on a daily basis
- Perform encryption
- Testing procedures: ex: data, network, systems, the operational impact of security breaches, WANs, intranets, wireless access systems.

P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.

- Firewall.

Firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predefined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network, such as the internet

  - Content filtering:
  - Signature identification:
  - Virus scanning services:
  - Network Address Translation (NAT):
  - URL filtering:
  - Bandwidth management:

- Intrusion Detection System (IDS).

IDS is a system that detects signs of intrusion attacks and can initiate actions on other devices to prevent attacks. Unlike firewalls, IDS does not prevent access but only monitors activities on the network to find out the signs of attack and alert the network administrator

  - How do intrusion detection systems work?
  - Possible responses to a triggered event:
  - Potential consequences of incorrect IDS configuration

P4 Show, using an example for each, how implementing a DMZ, static IP, and NAT in a network can improve Network Security.

- Demilitarized zone (DMZ).

Demilitarized zone, also referred to as the ring network, (DMZ). The DMZ is a part of the network where you position servers that must be available from the network's external and internal sources. Do not link to any network directly and it must still be reached through a firewall. The military term DMZ is used when a region of little to no compliance or control is described.

- Single firewall
- Dual firewall
- NAT (Network Address Translation)

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

- Static IP:

A static IP address is an IP address that is manually configured for the device, as opposed to an IP address assigned through a DHCP server. It is called a "static" address because it doesn't change. This is the complete opposite of dynamic IP addresses, which can be changed

  - Function:
  - Advantages of implementing static IP:

M1 Propose a method to assess and treat IT security risks

- Method to assess and treat risk
- Things that need security
  - Software:
  - About Software:
  - Data:
  - About Data:

M2 Discuss three benefits to implement network monitoring systems with supporting reasons.

- Conclusion

- What I've said so far, as well as specific examples, was intended to help people better understand information technology security, which is a critical task that will help the company grow more quickly. My lecture will include the processes and procedures for detecting and assessing IT security risks, as well as management measures for safeguarding confidential data and facilities in the workplace.
- LAN is the local network of an organization that is prevented from unauthorized attacks and intrusion by hackers from outside to protect the system data of a safe organization.