Presented by: Bùi Hương Linh
Class: GCH1002
Student ID: GBH200662
Tutor: Michael Omar

Security

Table of content

Task1: Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences

1. Define threats.

   Threats are security conditions that could have negative effects on people's lives or property. It could take the form of physical or verbal warnings intended to frighten a specific demographic.

2. Identify threats agents to organizations.

Organised crime: Criminals target personal data for a variety of reasons. Credit card fraud, identity theft, bank account fraud, and more. These crimes are now being carried out on an industrial scale. Methods vary from phishing attacks to "watering hole" sites, but the end result is the same. You and your data are extracted and used for malicious purposes.

3. List type of threats that organizations will face
   - Advanced Persistent Threats (APT)
   - Distributed Denial of Service (DDoS)

Task1: Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences

4. What are the recent security breaches? List and give examples with dates

- Define security breaches:

A security breach is an incident that causes unauthorized access to computer data, applications, networks, or devices. This leads to unauthorized access to information. Usually occurs when an intruder is able to bypass security mechanisms.

- Types of security breaches:

Access can also be obtained using social engineering. For example, an intruder calls a company pretending to be her IT helpdesk employee and asks for a password to "fix" a computer.

5. Discuss the consequences of this breach

The impact on organizations exposed to data breaches is severe and growing. This is primarily due to the increased regulatory burden of notifying individuals whose data has been compromised.

6. Suggest solutions to organizations

-You can maintain perimeter security and other protections, but you also need a data-centric solution that allows you to precisely control who can read specific files and records. Encryption gives you that kind of control, but it has to be the right kind of encryption.

Task 2 - Describe at least 3 organizational security procedures

1. What is security procedures?

Security procedures are detailed instructions for implementing, enabling, or enforcing the security controls outlined in your organization's security policy. Security procedures should cover the many hardware and software components that support business processes, as well as all security-related business processes themselves (such as onboarding new employees and assigning access rights).

2. Some organizational security procedures.

- Acceptable Use Policy (AUP):
- Access Control Policy (ACP):
- Business Continuity Plan (BCP):
- Disaster Recovery Policy:

Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS

1. Discuss briefly firewalls and policies, their usage and advantages in a network.

- Firewall defined

A firewall is a type of network security device that monitors incoming and outgoing network traffic and allows or denies data packets based on a set of security rules. Its purpose is to create a barrier between your internal network and incoming traffic from outside sources (such as the internet) in order to prevent malicious traffic such as viruses and hackers.

- Advantages of firewalls
  - Stops spyware
  - Promotes privacy
  - Prevents hacking
  - Stops virus attacks
  - Monitors network traffic

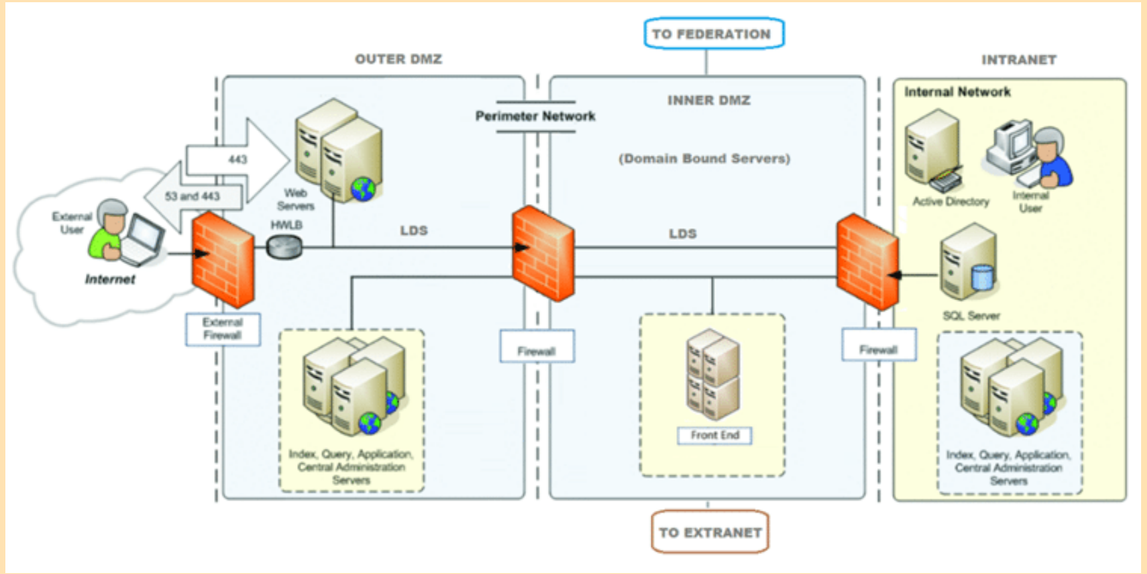
2. How does a firewall provide security to a network?

- Software firewalls
  - Firewalls use different methods to protect your network or computer:
    + Packet filtering
    + Proxy service
    + Stateful inspection
- Hardware firewalls
  - A hardware firewall is a system that works independently of the computer it is protecting by filtering information entering the system from the internet. A broadband internet router will almost certainly have its own firewall.

Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS

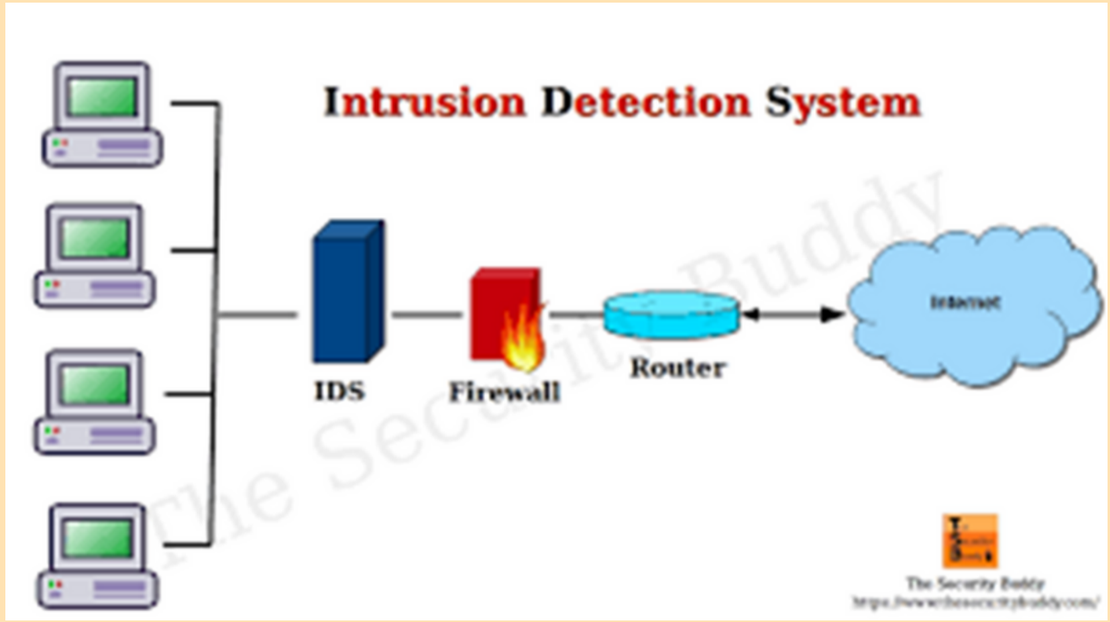
3. How firewall works

First, the firewall system analyzes network traffic based on rules. A firewall only welcomes incoming connections that it is configured to accept. It does this by allowing or blocking specific data packets (units of communication sent over digital networks) based on predefined security rules.



4. Define IDS

An intrusion detection system (IDS) is a network security technology originally designed to detect the exploitation of vulnerabilities on targeted applications or computers. Intrusion prevention systems (IPS) have enhanced IDS solutions with the ability to block threats in addition to detection, and have become the primary deployment option for IDS/IPS technology.



Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS

5. Firewall and IDS if they are incorrectly configured in a network

- Firewall
  + Firewall issues are one of the main reasons this is the case.
  + Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.
  + Rapid change and accelerating hybrid cloud adoption make network security difficult to maintain.
  + Many organizations try to protect themselves with network firewalls, increasing the risk of configuration errors and policy gaps.

- IDS

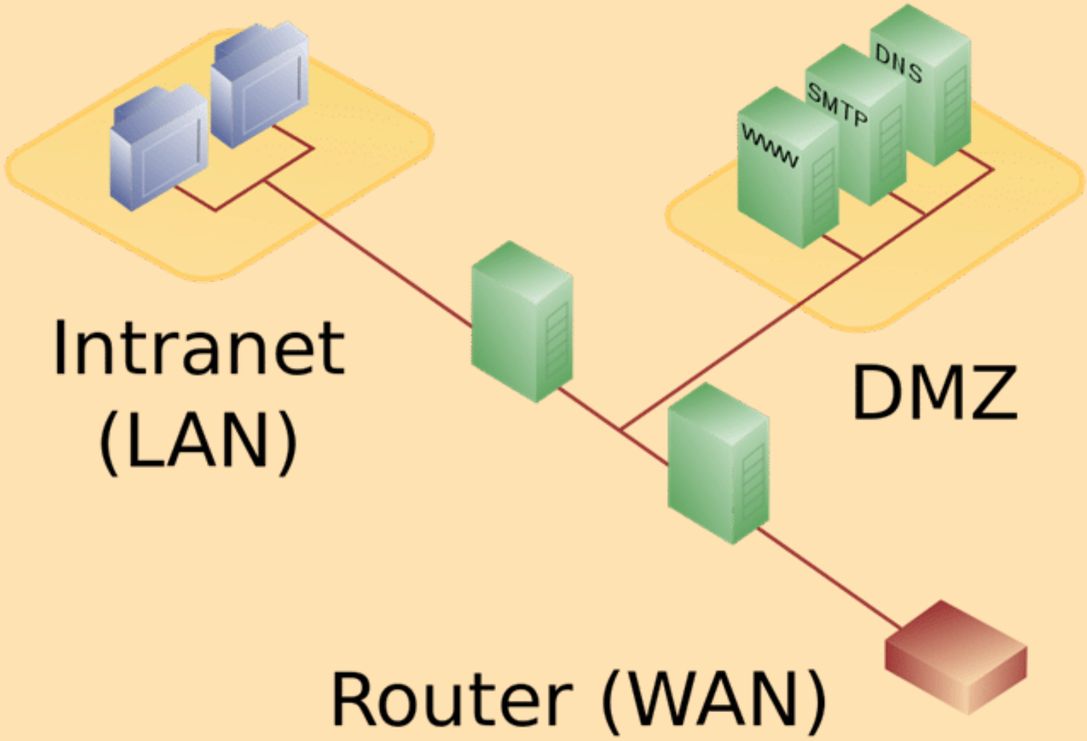
  IDSs are prone to false positives (or false positives). As a result, the company has to make fine adjustments during the initial installation of his IDS product. This includes properly configuring intrusion detection systems to compare normal traffic on your network with potentially malicious activity.

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security

1. Define and discuss DMZ

- What is DMZ?

A DMZ network is a perimeter network that protects an organization's internal local network from untrusted traffic and provides an additional layer of security. A shared DMZ is a subnetwork between the public internet and a private network.



- Benefits of DMZs

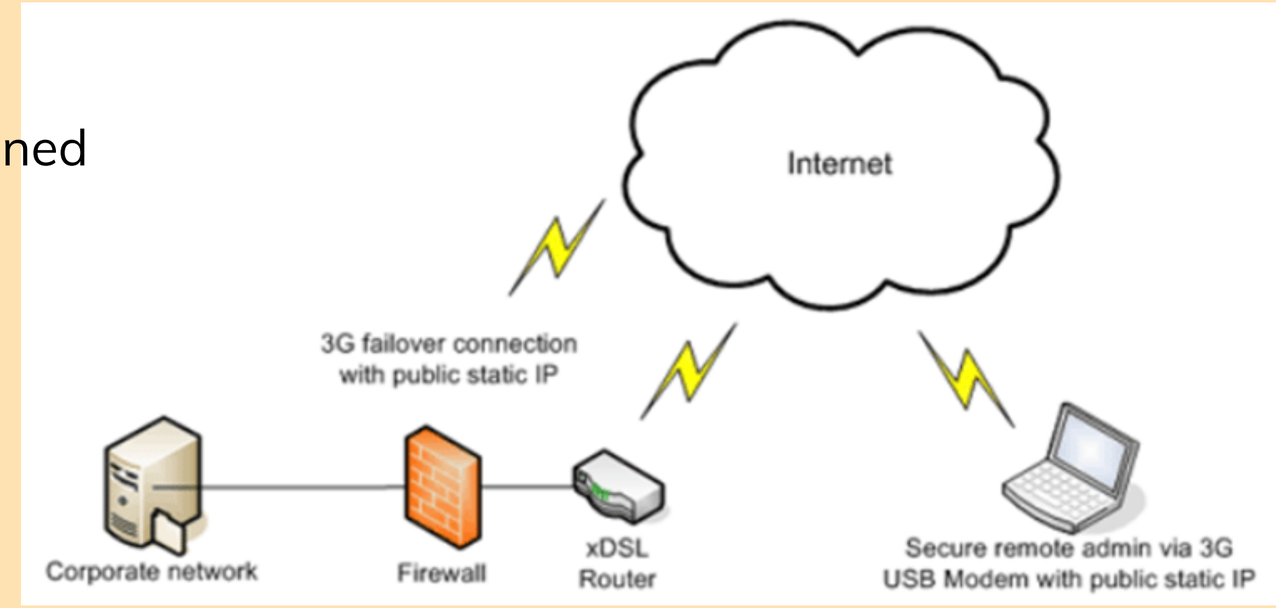
- Enable access control
- Prevent network reconnaissance
- Block Internet Protocol (IP) spoofing

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security

2. Define and discuss static IP

- What is static IP?

A static IP address is an IP address that is manually configured for a device and not assigned by a DHCP server. It is called static because it does not change, unlike a dynamic IP address, which changes.



- Benefits of IP addresses

- Speed
- Security
- Accessibility
- Hosting
- Stability
- Accuracy
- Shared Resource

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security

3. Define and discuss NAT

- What is NAT?

Network Address Translation (NAT) is the process of mapping one Internet Protocol (IP) address to another IP address by modifying the IP packet headers while in transit through a router. This improves security and reduces the number of IP addresses your organization needs.

- Benefits of NAT

- - This allows you to recover your private IP address
- It has excellent security features that enhance the security of private networks by isolating the internal network from the external network
- -Helps conserve IP address space. A large number of hosts can be connected to the global Internet using a small IP address.

References

BISSON, D., 2022. 5 Ways Your Organization Can Ensure Improved Data Security. [Online]
Available at: https://www.tripwire.com/state-of-security/security-data-protection/5-ways-you-can-ensure-improved-data-security/
Burton, D., 2020. The Dangers of Firewall Misconfigurations and How to Avoid Them. [Online]
Available at: https://www.akamai.com/blog/security/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them
CloudMask , 2022. Data Breaches: Threats and Consequences. [Online]
Available at: https://www.cloudmask.com/blog/data-breaches-threats-and-consequences#:~:text=Depending%20on%20the%20type%20of,and%20possibly%20compensate%20those%20affected.
DUNHAM, R., 2018. Security Procedures – How Do They Fit Into My Overall Security Documentation Library?. [Online]
Available at: https://linfordco.com/blog/security-procedures/?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g
Forcepoint, 2022. What is a Firewall?. [Online]
Available at: https://www.forcepoint.com/cyber-edu/firewall?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g

Thank for listening