SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Sabotage-Internal treats, Environmental threats

sabotage

- Sabotage in **networking refers to intentional actions** taken by someone to disrupt or damage a network's normal functioning. Sabotage can take many forms, including:

1.Physical damage to network equipment: This could include cutting network cables, damaging routers, switches, or other network devices.

2.Unauthorized access: A person may attempt to gain unauthorized access to the network or use someone else's credentials to access sensitive

3. **Malware and viruses:** Malware and viruses are programs designed to cause damage to a network, including stealing sensitive data, destroying files, and disrupting the network.
4. **Denial of Service (DoS) attacks:** A DoS attack is a type of cyber attack that floods a network with traffic, overwhelming it and causing it to crash.
5. **Social engineering:** Social engineering is a tactic where attackers trick people into providing sensitive information or performing actions that are not in the best interest of the network.

- It is **important to implement security measures** to protect against sabotage in networking.

- This includes **restricting physical access to network equipment**, implementing firewalls and intrusion detection systems, regularly updating software and security patches, and educating employees on how to identify and prevent social engineering attacks.

Internal threats

- Internal threats in networking refer to **security risks** that originate from within an organization or network.

- These types of threats can be **particularly dangerous** because they can be caused by employees, contractors, or other insiders who have authorized access to the network, and can often go undetected for extended periods.

- examples of internal threats in networking:

1. **Insider attacks:**

- This is when an **authorized user intentionally misuses** their access privileges to **steal sensitive data** or cause damage to the network.
- Insider attacks can take many forms, **including stealing passwords, installing malware or spyware, or manipulating data for financial gain**.

2.**Accidental data leaks:**

- This is when an employee **unintentionally exposes sensitive data, either through email, file sharing, or other means.**
- Accidental data leaks can be caused by something as simple as a **misaddressed email or a lost USB drive.**

3.Unintentional malware or virus infections:

- This is when an employee unknowingly introduces malware or a virus onto the network, which can then infect other machines and cause significant damage.

- To mitigate internal threats, organizations should implement access controls and user permissions, perform regular audits of user activity, provide employee security awareness training, and use security monitoring tools to detect any unusual behavior on the network.

- It is also important to have policies and procedures in place for incident response and to conduct regular vulnerability assessments to identify and address potential security weaknesses.


Network Security Threats
Human Threats
Physical Security Threats
Software Threats
WHAT ARE INTERNAL THREATS?
Legal Threats
Communication Security Threats
Other Threats
Social & Economic Threats

Environmental threats

- Environmental threats in networking refer to **security risks** that originate from the **physical environment surrounding the network**.

- These types of threats can be unpredictable and can cause significant damage to the network infrastructure, disrupt network availability, and compromise the security of data.

- common examples of environmental threats in networking:

1.Natural disasters:

- Natural disasters like floods, hurricanes, earthquakes, and wildfires can damage network infrastructure, power outages, and interrupt network connectivity.
- This can cause data loss, equipment failure, and downtime that can impact an organization's ability to operate.

2.Power outages:

- Power outages can disrupt network availability and cause data loss or corruption.

- They can also damage network equipment and cause unexpected downtime, which can be costly for an organization.

3.Temperature and humidity:

- High temperatures and humidity can damage network equipment, leading to equipment failure and data loss.

- Similarly, low temperatures can cause equipment to malfunction or stop working entirely.

- To mitigate environmental threats, organizations can implement physical security measures like backup power sources, uninterruptible power supplies (UPS), fire suppression systems, and redundant network connections.

- Regular maintenance of equipment, such as cleaning and monitoring temperature and humidity levels, can also help prevent damage from environmental threats.

- Additionally, organizations should have contingency plans in place for disaster recovery and business continuity to ensure that they can recover from unexpected events and minimize the impact on their operations.


External Suppliers
Poor Defence
Outdated Software
WHAT ARE EXTERNAL THREATS?
Cyber Attack
Exploitation
Social Engineering

Any Query????

Thank you……