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 V-CYBER ANALYSIS

Topic : Cyber security design and maintaining resilience

Cyber security design and maintaining resilience

- Cybersecurity design and maintaining resilience are **critical components** of any **organization's information security strategy**.
- The design of a cybersecurity system should be based on an **understanding of the potential threats, vulnerabilities, and risks that the organization may face**, and should be **tailored to the specific needs and goals** of the organization.

IMPORTANCE ELEMENTS

Risk assessment

- A risk assessment should be conducted to **identify potential vulnerabilities and threats** to the organization's information systems. This should include an analysis of the potential **impact of a cyberattack**, as well as the likelihood of such an attack occurring.

Security policies and procedures:

- Once potential risks have been **identified, policies and procedures** should be put in place to help mitigate those risks. This should include policies around **password management, access controls, data backups, and incident response.**

Training and awareness

- Employees are often the **weakest link in an organization's cybersecurity defenses**. **Training and awareness programs** should be put in place to educate **employees about cybersecurity best practices** and how to identify potential threats.

Technical controls

- Technical controls are the **mechanisms that are put in place to enforce security policies**. These can include **firewalls, intrusion detection and prevention systems, anti-malware software, and encryption.**

Five principles for the design of cyber secure systems

- **1. Establish the context before designing a system**

•Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified short-comings.

- **2. Make compromise difficult**

•Designing with security in mind means applying concepts and using techniques which make it harder for attackers to compromise your data or systems.

- **3. Make disruption difficult**

•When high-value or critical services rely on technology for delivery, it becomes essential that the technology is always available. In these cases the acceptable percentage of ‘down time’ can be effectively zero.

- **4. Make compromise detection easier**
- Even if you take all available precautions, there's still a chance your system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, you should be well positioned to detect compromise.
- **5. Reduce the impact of compromise**
- Design to naturally minimize the severity of any compromise.

What is Cyber Resilience?

- **Maintaining resilience involves ensuring that an organization's cybersecurity defenses remain effective over time.**
- **This can be achieved through the following strategies:**

Continuous monitoring

- Cyber threats are constantly **evolving, and organizations** must continuously monitor their systems for potential threats and vulnerabilities.

Regular updates and patches

- Cybersecurity **software and hardware** must be kept up to date with the latest patches and updates to ensure that they remain effective.

Penetration testing

- Penetration testing involves **testing an organization's cybersecurity defenses** by **attempting to simulate a real-world attack**. This can help **identify weaknesses in the system** and enable the organization to take corrective action.

Incident response planning

- Incident response planning involves preparing for the **worst-case scenario** by developing a plan for responding to a **cybersecurity breach**. This should include procedures for containing **the breach, identifying the cause, and restoring normal operations as quickly as possible**.


Confidentiality
Integrity
Utility
Authenticity
Information quality
& validity
System configuration
Availability
Safety
Resilience
Continuity of
operations
Safety of personnel
& assets
Possession
Controlling access
& system operations

7 Steps to cyber resilience:

- Identify risk.
- Test critical systems.
- Incident simulation.
- Assess organisational fitness.
- The redundancy principle.
- Measure reality.

Any Query????

Thank you……