Class 7 - 30/08/2023

Task - CIS Top 20 Critical Security Controls

The CIS Controls, is a set of best practices designed to help organizations improve their cybersecurity posture and defend against the most common and impactful cyber threats.

Basic CIS Controls

The first group of CIS critical security controls is known as the basic controls. The wider cybersecurity community often refers to these controls as **"cyber hygiene"** as it is something that should be done continuously and as a practice of maintaining the organization's cyber-health.

1. **Inventory and Control of Hardware Assets**:
   Establish and maintain an accurate inventory of authorized devices, their configurations, and connections to the network. This control helps prevent unauthorized devices from accessing the network.
2. **Inventory and Control of Software Assets**:
   Establish and maintain an accurate inventory of authorized software applications, and ensure that only approved software is allowed to run on systems.
3. **Continuous Vulnerability Management**:
   Regularly assess and remediate vulnerabilities in systems, applications, and network devices to reduce exposure to cyber threats.
4. **Controlled Use of Administrative Privileges**:
   Limit and monitor administrative access to systems and applications. Only authorized individuals should have administrative privileges, and those privileges should be tightly controlled.

5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**:
   Apply secure configurations to all devices, ensuring that systems are properly configured to minimize vulnerabilities and attack surfaces.
6. **Maintenance, Monitoring, and Analysis of Audit Logs**:
   Ensure that logging mechanisms are in place to track events on systems and networks. Regularly review and analyze logs to detect and respond to suspicious activities.

Foundational CIS Controls

The foundational CIS critical security controls number 7-15. These controls are more technical than the basic controls and involve more specific measures.

1. **Email and Web Browser Protections**:
   Employ email and web browser security controls to defend against phishing attacks, malicious attachments, and malicious websites.
2. **Malware Defenses**:
   Implement anti-malware measures to detect, prevent, and remediate malicious software infections across the organization's infrastructure.
3. **Limitation and Control of Network Ports, Protocols, and Services**:
   Minimize network attack surfaces by only enabling essential network services and protocols. Disable unused or unnecessary ports and services.
4. **Data Recovery Capabilities**:
   Establish data backup and recovery procedures to ensure that critical information can be recovered in the event of data loss or system compromise.
5. **Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches**:
   Implement secure configurations on network devices to reduce potential vulnerabilities and ensure proper network traffic filtering.
6. **Boundary Defense**:
   Implement measures to detect and prevent unauthorized access and data

exfiltration at network boundaries. This includes firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS).

7. **Data Protection**:
   Encrypt sensitive information at rest and in transit. Utilize data loss prevention (DLP) solutions to prevent unauthorized data sharing.
8. **Controlled Access Based on the Need to Know**:
   Limit user access to data and systems to only what is necessary for their roles. This minimizes the potential impact of insider threats and unauthorized access.
9. **Wireless Access Control**:
   Secure wireless networks by implementing strong authentication and encryption mechanisms to prevent unauthorized access.
10. **Account Monitoring and Control**:
    Continuously monitor user accounts and activities for signs of unauthorized or malicious actions.

Organizational Controls

The organizational controls consist of the last four CIS critical security controls. This group is focused on the strategic implementation of cybersecurity by design, intended to create a culture of cybersecurity within the organization.

1. **Implement a Security Awareness and Training Program**:
   Provide regular cybersecurity education and training to all employees, helping them recognize and respond to security threats.
2. **Application Software Security**:
   Ensure that application software is developed and tested with security in mind. Regularly update and patch applications to mitigate vulnerabilities.
3. **Incident Response and Management**:
   Develop an incident response plan to effectively detect, respond to, and recover from cybersecurity incidents.
4. **Penetration Testing and Red Team Exercises**:
   Regularly conduct penetration tests and simulated attacks (red team exercises) to

identify and address vulnerabilities before attackers can exploit them.