TASK 4

Overview

Write about the CIS controls and elaborate on them.

CIS Controls

The Center for Internet Security (CIS) Controls, formerly known as the SANS Top 20 Critical Security Controls, is a set of best practices designed to help organizations enhance their cybersecurity posture. These controls provide a prioritized approach to strengthening security and managing cyber risks effectively. The CIS Controls are organized into three categories: Basic, Foundational, and Organizational. Each of them is as follows:

Basic CIS Controls:

1. Inventory and Control of Hardware Assets:

Organizations should maintain an up-to-date inventory of all hardware devices, including servers, workstations, and mobile devices. This control ensures that no unauthorized devices are connected to the network, reducing the attack surface.

2. Inventory and Control of Software Assets:

Like hardware assets, software assets must be inventoried and maintained. Unauthorized and outdated software can introduce vulnerabilities, making software asset management critical.

3. Continuous Vulnerability Management:

This control involves identifying, tracking, and remediating vulnerabilities in a timely manner. Regular vulnerability scanning and patch management processes are essential.

4. Controlled Use of Administrative Privileges:

Administrative accounts should be restricted to a limited number of authorized individuals. This control helps prevent misuse and abuse of high-level access.

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:

Enforcing secure configurations on all devices helps reduce the attack surface and minimizes potential vulnerabilities. This includes settings for operating systems, applications, and services.

6. Maintenance, Monitoring, and Analysis of Audit Logs:

Logging is crucial for identifying and responding to security incidents. Organizations should configure and maintain logs, analyze them regularly, and retain them for an appropriate duration.

Foundational CIS Controls:

1. Email and Web Browser Protections:

Implement protections in email and web browsers to block malicious content and phishing attacks. These controls enhance user security awareness.

2. Malware Defenses:

Organizations should implement anti-malware measures, including antivirus, anti-spyware, and intrusion detection/prevention systems, to protect against malware.

3. Limitation and Control of Network Ports, Protocols, and Services:

Reducing the number of open ports, protocols, and services minimizes the attack surface. This control is crucial for network security.

4. Data Protection:

This control involves encryption, access controls, and monitoring of sensitive data. Protecting data at rest and in transit is vital to prevent data breaches.

5. Secure Configuration of Network Devices, such as Firewalls, Routers, and Switches:

Securely configuring network devices helps prevent misconfigurations that could expose the network to attacks or allow unauthorized access.

6. Boundary Defense:

Organizations should establish and monitor network boundaries, implementing firewalls and intrusion detection systems to detect and block malicious activity at the network perimeter.

Organizational CIS Controls:

1. Data Protection:

This control involves encryption, access controls, and monitoring of sensitive data. Protecting data at rest and in transit is vital to prevent data breaches.

2. Controlled Access Based on the Need to Know:

Implementing strict access controls ensures that individuals only have access to the data and resources required for their job roles.

3. Wireless Access Control:

Organizations should secure wireless networks, implementing strong authentication and encryption measures to protect against unauthorized access.

4. Account Monitoring and Control:

Monitoring and controlling user accounts, especially privileged accounts, helps detect and prevent unauthorized activities.

5. Security Skills Assessment and Appropriate Training to Fill Gaps:

Organizations should invest in cybersecurity training for their staff, ensuring they have the skills and knowledge to defend against evolving threats.

6. Incident Response and Management:

Having an incident response plan and processes in place is critical. Organizations should be prepared to detect, respond to, and recover from security incidents efficiently.

7. Secure Network Engineering:

Secure network engineering ensures that network infrastructure is designed and configured with security in mind, reducing vulnerabilities and attack vectors.

8. Penetration Testing and Red Team Exercises:

Regularly testing the organization's defenses through penetration testing and red team exercises helps identify weaknesses and assess the effectiveness of security controls.