TASK 4 (30-08-23)

Overview of the assignment : Write about the CIS controls and elaborate on them.

What are 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 and guidelines for cybersecurity. These controls are designed to help organizations improve their overall cybersecurity posture by providing a prioritized framework of actions to mitigate the most common and damaging cyber threats.

There are currently 20 CIS controls organized into three implementation groups :

Basic

1.Inventory and Control of Hardware Assets
2.Inventory and Control of Software Assets
3.Continuous Vulnerability Management
4.Controlled Use of Administrative Privileges
5.Secure Configuration for Hardware and Software
6.Maintenance,Monitoring and Analysis of Audit logs

Foundational

7.Email and Web Browser Protections
8.Malware Defenses
9.Limitation and Control of Network Ports, Protocols, and Services
10.Data Recovery Capabilities
11.Secure Configuration for Network Devices
12.Boundary Defense
13.Data Protection
14.Controlled Access Based on the Need to know
15.Wireless Access Control
16.Account Monitoring and Control

Organizational

17.Implement a security awareness and training program
18.Application Software security
19.Incident Response and Management
20.Penetration tests and Red Team Exercises

1.Inventory and Control of Hardware Assets : Know what devices are on your network. Keep a list of all the computers, servers, and other hardware that are connected to your organization's network. This way, you can manage and secure them effectively.

2.Inventory and Control of Software Assets : Keep track of the software you use. Maintain a list of all the software applications installed on your systems. This helps you ensure that you're using legitimate and up-to-date software.

3.Continuous Vulnerability Management : Stay updated and fix problems. Regularly check for security vulnerabilities in your software and systems. When you find vulnerabilities, fix them quickly to prevent hackers from exploiting them.

4.Controlled Use of Administrative Privileges : Limit power, reduce risk. Only give administrative access to people who really need it. This reduces the risk of unauthorized changes that could harm your systems.

5.Secure Configuration for Hardware and Software : Set things up securely. Ensure that your hardware and software are configured in a way that makes them as secure as possible. This minimizes potential security weaknesses.

6.Maintenance,Monitoring and Analysis of Audit logs : Regularly check and maintain the records of system and network activities. Ensure that logs are generated, stored securely, and retained for a sufficient period.

Continuously watch these logs for unusual or suspicious activities. It's like having a security guard who keeps an eye on your property for any signs of trouble.When you see something unusual or potentially harmful in the logs, investigate it. Think of this as reviewing security footage to understand what happened and whether it poses a threat.

7.Email and Web Browser Protections: Safeguard your digital mail and windows to the internet. Put measures in place to protect your employees from malicious emails and websites. Just like you wouldn't open a suspicious-looking letter or visit a sketchy website, ensure that your email and web browsing activities are secure.

8.Malware Defenses: Guard against digital infections. Use antivirus and anti-malware tools to protect your systems from malicious software, just like you would use hand sanitizer to protect yourself from germs.

9.Limitation and Control of Network Ports, Protocols, and Services: Control the doors and windows to your digital house. Limit the ways in which information can enter or exit your

network. Think of this like locking some doors and windows in your home to prevent unauthorized access.

10.Data Recovery Capabilities: Just like you have a spare key hidden in case you get locked out of your home, data recovery capabilities are like having a backup plan for your digital information. It means being able to retrieve your important data when something goes wrong, such as a cyberattack, hardware failure, or accidental deletion.

11.Secure Configuration for Network Devices: Set up your digital devices securely. Ensure that routers, switches, and other network equipment are configured in a way that makes them as secure as possible, just like you would lock the doors and windows of your house properly.

12.Boundary Defense: Secure your digital perimeter. Implement security controls at the edge of your network to protect against external threats, similar to having a fence or security system around your physical property.

13.Data Protection: Think of data protection as safeguarding your digital secrets..Guard your sensitive information. Put safeguards in place to protect important data, such as customer information or trade secrets, from unauthorized access or theft.

14.Controlled Access Based on the Need to know : Just as you wouldn't share your personal diary with everyone, in the digital world, you limit access to sensitive information only to those who genuinely require it for their job or tasks.It's like giving someone access to the parts of your house they need to do their job but not giving them access to your entire property. Apply the same principle in your digital environment, granting the least privilege necessary for each role.

15.Wireless Access Control: Picture your Wi-Fi network like a front door with a lock. Wireless access control is like deciding who gets a key to that door. You want to make sure that only authorized users can connect to your Wi-Fi network and use it securely.

16.Account Monitoring and Control: Think of your digital accounts, like email or social media, as locked rooms. Account monitoring and control are like checking who has keys to those rooms and making sure only the right people can enter.

17.Implement a security awareness and training program: Similar to teaching your family about home safety, security awareness and training is about educating your employees and users on cybersecurity best practices. It helps them recognize and respond to digital dangers, just like you'd teach your family to be cautious about strangers or potential risks in your neighborhood.

18.Application Software security: Imagine your computer software as the various appliances and tools you have in your home. Application software security is like ensuring that these tools are safe to use and won't cause harm.

19.Incident Response and Management: Incident response and management is like having a plan in place for emergencies at home. It's about having a clear process to follow when something goes wrong in your digital environment, whether it's a security breach or a technical issue. Just as you'd have a fire escape plan, you need a plan for digital emergencies.

20.Penetration tests and Red Team Exercises: Penetration testing and red team exercises are like hiring a professional locksmith to test the security of your home's locks. It involves simulating cyberattacks to find weaknesses in your defenses before real attackers can exploit them.