Understanding CIS policies

Basic:

1.Inventory and control of Hardware assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

2.Inventory and control of software assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

3.Continious Vulnerability Management:

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

4.Controlled use of administrative privileges:

The focus of this control is to ensure that all users with administrative level access use a dedicated or secondary account for any elevated activity. This administrator account should not be used for any other purpose, and should not be used for email, web-browsing, or similar activity.

5.Maintenance, Monitoring and Analysis of Audit logs:

Maintenance, Monitoring and Analysis of Audit logs of events that could help detect, understand, or recover from an attack.

Foundational:

7.Email and Web Browser Protections:

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

8.Malware Defences:

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

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

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

10. Data Recovery Capabilities:

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

11.Secure Configurations for Network Devices, such as Firewalls, Routers, and Switches:

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

12.Boundary Defence:

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

13. Data Protection:

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

14.Controlled Access Based on the Need to Know:

The focus of this control is to ensure users are only allowed access to information they are authorized or needed to perform job duties. There are several layers to this complex problem, beginning with network segmentation, and growing to data classification and Data Loss Prevention (DLP) products.

15.Wireless Access Control:

The focus of this control is to ensure wireless access is configured to track and control access, prevent unauthorized access. If misconfigurations are found, the settings should be corrected. Wireless access has become a common and natural part of a majority of organizations network infrastructure. Wireless access is beneficial, but exposes networks to problems related to network boundaries, all of which come back to this basic series of questions:

16.Account Monitoring and Control:

The focus of this control is to ensure that all accounts are managed in a fashion that promotes clean account hygiene. This misuse or neglect of account maintenance can lead to system compromise.

Organizational:

17.Implement a Security Awareness and Training Program:

The security awareness program is influenced by the maturity of an organization. For example, a small company with 100 employees or less can have a very informal program, while a fortune 500 company on average has over 60,000 employees and must have a very formal program.

18. Application Software Security:

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

19.Incident Response and Management:

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

20.Penetration Tests and Red Team Exercises:

Test the overall strength of an organization’s defence (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.