UNDERSTANDING CIS POLICIES

BASICS:-

Inventory and Control of Hardware Assets

Control 1 helps the CIS to actively manage (inventory, track, and correct) all hardware devices on the network. This ensures only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Inventory and Control of Software Assets

The focus of this control is to actively manage (inventory, track, and correct) software installed on systems within the organization. A fundamental aspect of risk management is discovering risk by tracking software present on information systems. Ensuring only authorized software is used by the organization will increase the effectiveness of risk management efforts. Being able to quickly identify unauthorized and unmanaged software can prevent security breaches and increase the productivity of users.

Continuous Vulnerability Management

The focus of this control is to have an established vulnerability management program that is configured to conduct regular, comprehensive, credentialed scans across the organization. The most effective vulnerability scanning programs not only identify vulnerabilities, but also evaluate and report on a number of other critical concerns such as:

- Security configurations of systems
- Misconfigurations
- Unauthorized changes

- Patch levels of systems

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.

Secure Configuration for Hardware and Software

The focus of this control is to maintain documented security configuration standards for all authorized operating systems and software. Organizations must establish a baseline security configuration, implement a configuration management and change control process, and actively be able to report on the security configuration of all endpoint devices such as:

- Mobile devices
- Laptops
- Servers
- Workstations

Maintenance, Monitoring and Analysis of Audit Logs

The focus of this control is to collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

FOUNDATIONAL:-

Email and Web Browser Protections

The focus of this control is to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Malware Defenses

The focus of this control is to control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Limitation and Control of Network Ports, Protocols, and Services

The focus of this control is to 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. A common denominator is that attackers will always search for, and attempt to exploit, accessible and vulnerable network services. The most common attacks are generally against hosts such as web servers, mail servers, file and printer servers, etc.

Data Recovery Capabilities

The focus of this control is to ensure that the processes and tools used to properly back up critical information are in place within the organization and a proven methodology for timely recovery of data exists.

Secure Configuration for Network Device

The focus of this control is to 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.

Boundary Defense

The focus of this control is to ensure that the entry points into the network are clearly defined and monitored. Network boundaries in today's environment do not have a clear edge, and are typically no longer defined as a single ingress point protected by a firewall and edge routers of the past. Today, the network perimeter extends well beyond this gateway into the organization, and encompasses the cloud when using AWS, ASURE, or other services. A network edge is also the reach of a wireless network radio signal, and the VPN endpoints with more users working at home. This CISO must have a clear understanding of each network edge and the risks associated with each edge.

Data Protection

The focus of this control is to ensure that all data is classified and protected in accordance with established data classifications. To establish these data classifications, organizations should develop a list of the key data types and define the overall importance to the organization. This can be used to create a data classification scheme for the organization. Labels, such as "Sensitive," "Business Confidential", and "Public," should be used. The information owners need to be aware of the classification policy and the tools, procedures, and controls on said data.

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.

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

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:-

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.

Application Software Security

As an organization grows, custom applications are often developed to help with business workflow or other services which are offered to customers. These applications expose the organization to risk. Additionally, if the data stored is customer data, the customers may also be exposed. There are several tools in the market to help with Application Software Security. For example, the non-profit group provides information to aid in the detection and mitigation of such risk.

Incident Response and Management

A big part of a mature information security program is the Incidence Response (IR) program. The organization will grow into this practice as the size of the organization increases. However, the need for such a team remains constant. Many security incidents happen because a company is unaware of the asset or risk to the asset. The first and arguably most important step in vulnerability management is discovering assets, as risk can't be assessed, if the asset is unknown. Following all the preceding 18 CIS Controls will help bring awareness to the organization and the prepare the security team for the worst case scenario.

Penetration Tests and Red Team Exercises

As a final testament to a good security program, the CIS Control 20 recommends the organization test all the security controls. These exercises are very beneficial to training and security awareness. Many times well intended measures can be exploited. For example, a really strict password policy can result in users taping passwords to their keyboard. A great technical control, thwarted by a forgetful user and an observant adversary. Many times developers find protocols they find useful, and never realize there is an inherent security flaw, for example FTP and Telnet, are great tools. But in both cases, all credential exchanges are in clear text, allowing passwords and other information to be captured easily. Many chat programs use a form of HTTP and not HTTPS, again data is exchanged in the clear. With wireless technologies, many times with a simple wireless receiver, anyone can monitor the full exchanges of information. Penetration tests and red team exercises help to bring this information to the forefront of the security conversation.