CIS Controls

Version 8

By Dieubon Louima

Introduction

CIS stands for Center for Internet Security. It is a global community-driven nonprofit organization focus on developing guidance and best practices for securing IT systems and digital data. CIS lead by a community of IT professionals who continuously evolve standards and provide products and services to proactively safeguard against emerging threats.

CIS Controls formerly know as the SANS Critical Security Controls. Which are guidelines and best practices for securing IT infrastructures. By implementing these controls any organization could improve its security posture and prevent the most pervasive and dangerous attacks and also meet compliance requirements for most compliance frameworks out there.

In this presentation, I will go over each control and talk about what they are and why it is important to implement them.

CIS Control 1: Inventory and control of enterprise Assets

What is it ?

It is the process of keeping an active inventory list and manage all the company assets. It is included all the end-user devices, including portable and mobile, network devices; non-computing such as internet of things (IoT). It includes all devices connected to the infrastructure physically, virtually, remotely and those in the cloud environment.

Why do we do it?

One of the goal of security is to protect the company's assets and end-user devices. If one of these devices is unknown; it is not going to be possible to protect it. The CIS control 1 is about keeping an update list of all devices.

CIS Control 2: Inventory and Control of Software Assets

What is it ?

As in the control 1, you keep an inventory list of all physical devices. It is equally important to keep an active inventory list of all software, operating systems and applications of the enterprise network

Why do we do it?

It is important to track and controls all software running in the company infrastructure. And who can download and install software. It also helps detect unauthorized and unmanaged software and prevent them from running

CIS Control 3: Data Protection

What is it?

Data is one of the most valuable assets of the company. Keeping data protected should be everyone job. This control is to make sure to develop processes, technical controls to securely retain, classify and dispose of data

Why do we do it?

A company's data is also one of the most targeted assets by attackers. And companies rely on their data to be successful. Data breaches are very expensive and it is not handled correctly, the company risk to go bankrupt. Good data protection measures and controls are very important.

CIS Control 4: Secure Configuration of Enterprise Assets and Software

What is it ?

After having an active list of devices and software on the company's network. It is very important to make sure they have the proper configuration to allow them to communicate on the network. It includes all devices (network and end-user devices. non-computing/IoT and servers, software (operating system and applications)

Why do we do it?

Each device connected to the network is a potential entry point for an attacker. It is very important to make sure each one of these devices has proper configurations in order to keep the network safe. You need to make sure to close all unnecessary open ports and deactivated all unnecessary applications or software.

CIS Control 5: Account Management

What is it ?

It is very important to have and create processes, mechanisms,s, and tools to manage user accounts. Each account type (group) should be handled according to the level of privilege.

- Administration account
- User account
- Service account
- System account
-

Why do we do it?

Account management is very important to manage authentication and user authorization. And most importantly after a user is logging what permission do they have and what they can do with the data they have access to.

CIS Control 6: Access Control Management

What is it ?

An organization might have hundreds or even thousands of users with different permission sets accessing the network. Keeping track of all these users and permissions is tedious and even impossible to manage manually. That is where access control management comes into play. The organization needs some kind of access management tool to manage and automate these tasks. Such as

Create, assign, manage and revoke access and credentials.

Why do we do it?

Having good access control management is very important. It will help automatically to:

- Easily manage users (human, application, and third party application)
- Create users
- Grant and revoke access
- Enable multi-factor authentication for all users
- Manage remote access

CIS Control 7: Continuous Vulnerability Management

What is it?

An organization's network is made of different pieces of equipment, technologies, and software. They need to be set up, turned up, and synchronize to insure a well-working network. Unfortunately, these settings are easy to break due to third-party security patches, software updates, new features,s or even a simple workflow update.

An organization needs a good continuous vulnerability management implementation to help to stay ahead of the game.

Why do we do it?

Cybercriminals are constantly looking for vulnerabilities in an organization's infrastructure to exploit in order to gain access. Cyber defenders must have timely threat information available to them about the software updates, patches, security advisories, and threat bulletins to keep up with the latest information. And also cyber defenders must constantly scan and review their scan report to look for any vulnerability and fix it before an attacker find it and exploit it.

CIS Control 8: Audit Log Management

What is it?

Logs collection and analysis is very important for organization's ability to detect malicious activity and indicator of compromise.

Audit logs are machine data related to user-level events for example when a user logged in and accessed a file on the system. These logs are required planning and efforts to set them up.

Why do we do it?

Most of the time organizations collect and retain logs just for compliance purposes but they rarely analyze them. Attackers know that and they can take advantage of that to hide their activity on the system. That is why it is extremely important to collect and analyze machine data (logs) to detect any suspicious activities on the system.

Logs are also important for incident response.

CIS Control 9: Email Web Browser and Protections

What is it?

Email remains one of the most important tools for internal and external communication for any organization. It is also heavily used by attackers to deliver malicious codes to victim endpoints on an organization network. Email is a high target medium by attackers to manipulate human behavior through direct engagement.

Why do we do it?

Most ransomware attacks started due to a user click on a malicious link from an email received from the attacker. When that happens, it is game over. The victim's computer now is controlled by the attacker.

Emails make it very easy for the attacker's malicious code to run in the organization's network.

CIS Control 10: Malware Defenses

What is it?

A malware (virus or trojans) is a piece of malicious code running in the organization network or victim computer without the user's knowledge. A malware can performs diverse tasks such as capturing credentials, stealing data, delete or encrypting data.

That is why a good malware defends is extremely important to prevent installation, spread, and execution of malicious code, application, and script on the organization's assets.

Why do we do it?

Malware gets into the organization network or the victim's computer through a vulnerability in the system, email attachments, webpages, removal media, computers, and mobile devices.

CIS Control 11: Data Recovery

What is it?

Data is a critical asset for any organization. All decisions are based on available data if for some reason this data becomes unavailable or untrusted due to cyber attacks or disaster events the organization will not be able to run and make money.

That is why a good data recovery plan is necessary to restore an in-scope organization to a pre-incident and trusted state.

Why do we do it?

Cyber attacks are increasing in the last few years and natural disasters become more frequent as well. It is very important for the organization to have a good data recovery plan and process in place.

CIS Control 12: Network Infrastructure Management

What is it?

Network security is a constantly changing environment. It is necessary to constantly re-evaluate architecture diagrams, configuration, access control, and allowed traffic flows.

An organization needs good network infrastructure management to ensure a good defense against attackers. IT should be able to track, report, correct any network anomalies in a timely manner.

Why do we do it?

A good network infrastructure management should be able to perform regular vulnerability scan to identify any vulnerability such as default configuration, open service ports, default username and passwords, support for any vulnerable old protocol. Unsecure protocols, pre-installed software, inconsistent firewall rules, rogue access points, and unused open ports.

CIS Control 13: Network Monitoring and Defense

What is it?

Having a secure network and having a secure network configuration is not enough to fight against all the attack vectors. There should be also a good network monitoring and defense team dedicated to monitor and investigate network alerts and suspicious activity on the network.

Why do we do it?

The cyber threat landscape is changing and attackers are getting mature. The organization also needs to establish and maintain comprehensive network monitoring and defense against all these threats.

CIS Control 14: Security Awareness and Skills Training

What is it?

Users are known to be the weak points on the cyber defense. Users intentionally or unintentionally can cause cyber incidents due to mishandling sensitive data, using weak passwords, or sending emails with sensitive data to the wrong recipient. Or simply by losing an end-user device.

That is why establish and maintain a good security awareness training program could influence user behavior and make them more conscious about security and cybersecurity risks.

Why do we do it?

Any good cybersecurity program should start by securing potential entry points. One of these entry points is a user (human). To address this situation a good cybersecurity training program is needed. And the training program should be updated on a regular basis

CIS Control 15: Service Provider Management

What is it?

We are living a modern connected world and businesses rely heavily on third party vendor and partner infrastructures for core business application and functions.

There are a lot of sensitive information shared among these third party vendors and partners. Most data security and privacy regulations require data protection should be extended to third party service provider as well.

Why do we do it?

There are a lot of cyber breaches that occurred because the attackers have leveraged a vulnerability in third-party service providers or and actors in the supply chain. Third-party service provider management is crucial to make sure they meet certain standards and requirements for data security.

CIS Control 16: Application Software Security

What is it?

An enterprise might use several applications for core business functionality and meet business goals. These applications need to talk to each other and users with different permission need to access them as well. These applications run on top of other software and hardware as well.

It is important for the organization to manage the security life cycle of these applications.

Why do we do it?

These applications could be developed in-house, hosted in the cloud, or maybe third-party service providers. The organization should have application software management in place to help detect, remediate security weaknesses before they impact the organization network.

CIS Control 17: Incident Response Management

What is it?

A good and comprehensive cybersecurity program should include protections, detections, response, and recovery capabilities. The last two are commonly layout in an incident response plan. The organization should have a clear and concise plan to respond to any incident. Cyber breaches are occurring more frequently and it is no longer a matter if we get breached and become a matter of when we will get breached

Just in case that happens. The organization should be ready to detect, respond and recover.

Why do we do it?

The longer an attack remains undetectable on the organization network the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered.

CIS Control 18: Penetration Testing

What is it?

Good cybersecurity defense should be tested to see how effective and resilient is the system and to test the response plan. and the way to do that is through penetration testing.

Penetration testing is part of the reg team activity. They test and report the organization's security posture.

Why do we do it?

The main idea behind a penetration testing to identify potential vulnerability on the system before an attacker finds them and exploit them.

Reference

https://www.cisecurity.org/controls/inventory-and-control-of-enterprise-assets/

https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/

https://www.cisecurity.org/controls/data-protection/

https://www.cisecurity.org/controls/secure-configuration-of-enterprise-assets-and-software/

https://www.cisecurity.org/controls/account-management/

https://www.rapid7.com/fundamentals/cis-critical-security-controls/

https://www.tripwire.com/state-of-security/controls/cis-control-06/

https://controls-assessment-specification.readthedocs.io/en/stable/control-18/index.html