CIS Controls Version 8

K.H.

CIS Control 1: Inventory and Control of Enterprise Assets

What is inventory and control of Enterprise Assets

- Knowing what devices are on the network and what access/permissions they have are critical to enterprise network security.

Why is inventory and control of enterprise assests important?

- Hackers/attackers will constantly scan a network until an exploitable entry point is established. Once in a network, attackers can access sensitive data. Knowing what devices are on an Enterprise's network allows us to address any flaws and properly fortify all possible unwanted access points.

CIS Control 2
Inventory and Control of Software Assets

A thorough inventory and assessment of all software used on devices within an enterprise's network will make for a more well-protected network. Attackers' backdoor programs and bots allow them long-term control over systems by exploiting users who visit malicious websites and unknowingly download files used by attackers to gain control of a system and exploit possible program vulnerabilities. Updating and patching programs are critical in defending a network.

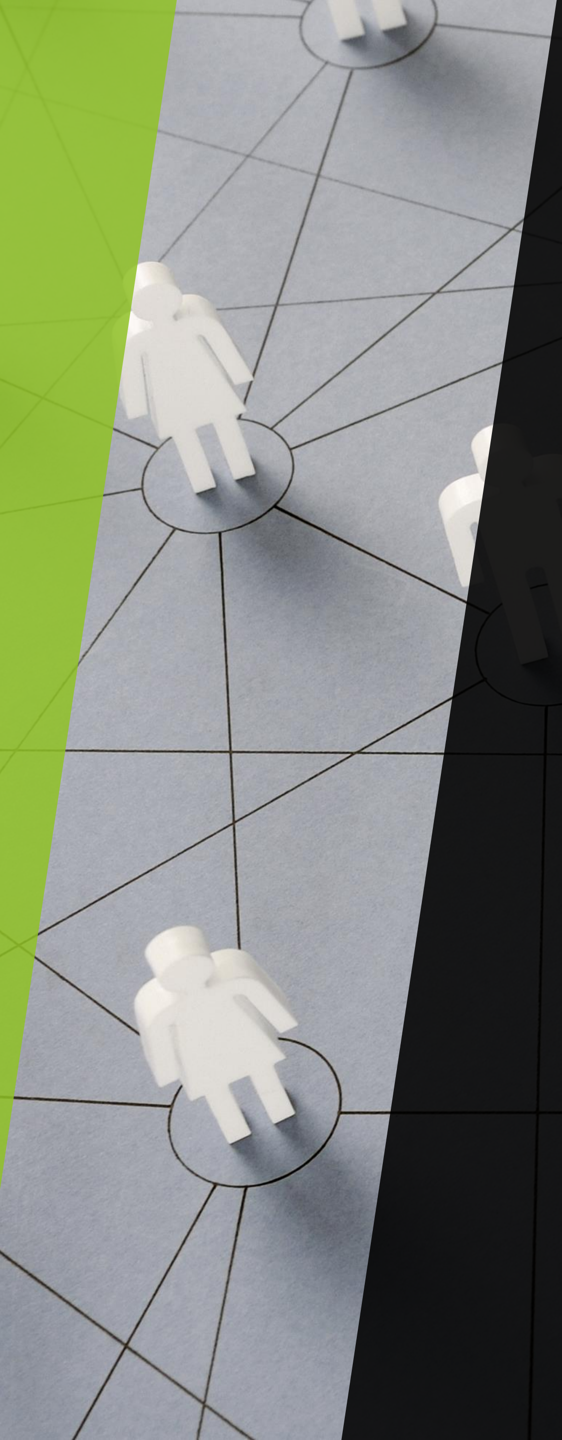
ACTIVELY MANGE SOFTWARE ON NETWORK.

INSURING ONLY APPROVED SOFTWARE (OPERATING SOFTWARE AND APPS). ENTERPRISE APPROVED

PREVENTING OF UNAPPROVED SOFTWARE AND REMOVAL OF UNAPPROVED SOFTWARE IF NECESSARY

CIS CONTROL 3: Data Protection

- Cis Control 3 - Data Protection
- - proper security, handling , management and disposal of data.
-
- Why is data protection important
- - To prevent attackers from extracting sensitive data of an enterprise, its employees and clients.



CIS CONTROL 4:
Secure Configuration of Enterprise Assets and Software

- What is secure configuration of enterprise assets and software?
  - create and manage a secure configuration for portable end user devices such as (Cell phones, tablets . Etc). Network devices; non- computing/Iot devices, servers and software (Apps and operating systems)

- Why is secure configuration of enterprise assets and software important?
  - Attackers will exploit unconfigured software and other enterprise assets

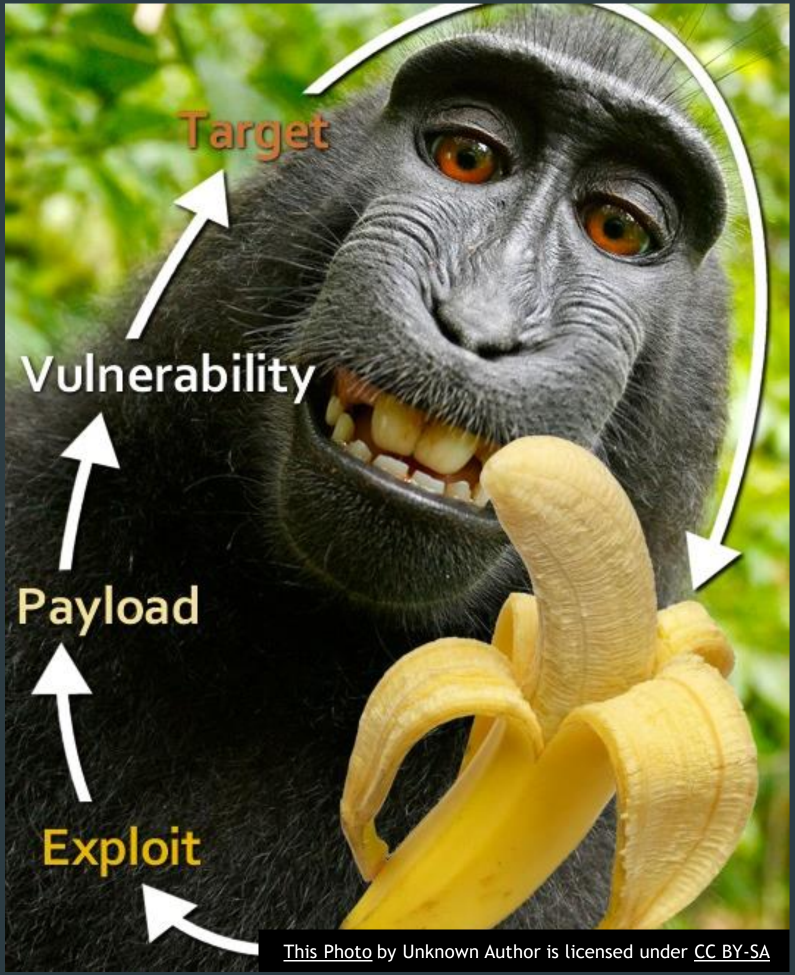
CIS Control 5:
Account Management

- Data for user accounts (Emails, user accounts, enterprise administration, service accounts, assets for and software) **should be protected using established processes and tools**.

- Why is CIS control 5 important ?
  - Attacker use account credential data to access to confidential and private information, disrupt services , and or gain control over systems.

CIS CONTROL 6:
ACESS CONTROL MANAGEMENT

- What is Access Control Management?
  - Tools and protocols designed to manage access, assign, remove and deny privileges for user in an enterprise.
- Why is access control management necessary?
  - User, administrators and clients only need the privileges necessary to what their role is in the enterprise. Unnecessary privileges given to user creates security risks that could’ve been easily prevented.



This Photo by Unknown Author is licensed under CC BY-SA

CIS CONTROL 7:
Continuous Vulnerability Management

- What is Continuous vulnerability management ?
  - - planned process to continuously observe track and manage vulnerabilities on devices in an enterprises network.
- Why is continuous vulnerability management important ?
  - continuous management of enterprise vulnerabilities is important in recovering from an attack and shrinking the window of a possible attack.

CIS CONTROL 8:
Audit Log Management

- What is Audit Log Management?
  - Log audit management is useful to track, retain, and review logs. \

- Why is Audit Log Management important?
  - Its is important to have audit log management when using logs to detect and understand attacks by "Hackers"

CIS CCONTROL 9:
Email and Web Browser Protections

- What is Email and Web Browser Protections?
  - It is the process of protecting against and detecting threats that come through email and web browsing.
- It is important to protect an Enterprise from web and email attacks.
  - Attackers will use web and email attacks to manipulate administrative privileges and or extract data.

CIS Control 10: Malware Defenses

- What is malware defense?
  - Prevention of unauthorized installation software, apps, and codes that may contain malicious content.
- Why is malware defense important?
  - Malware defense is important to Enterprise network integrity. Malware executable codes can disrupt an enterprises services and network functionality.

CIS Control 11: Data Recovery

What is data recovery ?

- The process of creating and storing a trusted state of an enterprise’s network.

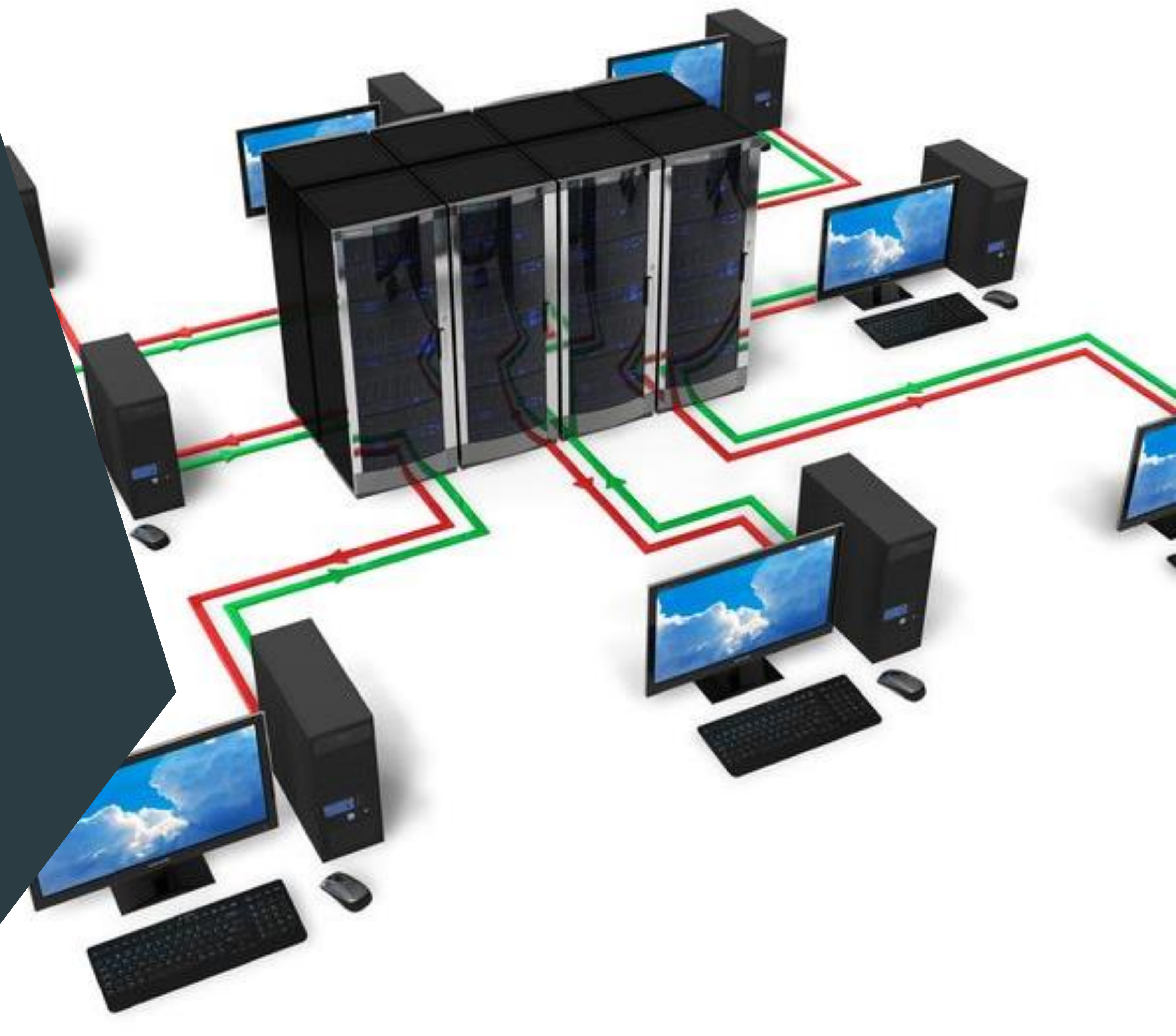
Why is data recovery important ?

- In the event of a successful attack, having a stored pre-incident state of the network allows an enterprise to return to a trusted functioning network.

CIS CONTROL 12: Network Infrastructure Management

- What is network infrastructure management ?
  - Tracking, reporting and correcting network devices. Attacker prevention. Identifying exploitable vulnerabilities.

- Why is network infrastructure management important
  - Network security is ever changing. Up to date network infrastructure is necessary to the integrity of a network as attacker will probe for inconsistences in routers, firewalls and switches rules.



CIS Control 13: Network Monitoring and Defense

- What is Network monitoring and defense?
  - Enterprise's network tools and software configuration used to monitor and protect against external attacks.
- Why is monitoring and defense important?
  - Attackers are persistent and their methods evolve. It is important keep a close watch on network security tools, they may need updating, patching and revised configuration.

CIS Control 14: Security Awareness and Skills Training

What is Security Awareness and Skills Training ?

- Established procedures to and guidelines geared to security awareness for employees and clients.

Why is Security Awareness and Skills Training important ?

- The easily influenced point of access into cyber network are the human users.

CIS Control 15: Service Provider Management

What is service provider management ?

- Service providers are often granted access to sensitive. Service providers may provide support of systems and processes used by Enterprise’s IT department.

Why is service provider management important/

- Service providers handle and manage data of Enterprise’s clients and employees. Its important have guidelines for how this information used and stored.

CIS Control 16: Application Software Security

What is application software security ?

- Security of Applications in a network. Software developed in the enterprise, acquired or hosted.

Why is application software security important ?

- Attackers can use Application software data (I.E., account credentials) to attack and compromise a network.

CIS Control 17: Incident Response Management

What is incident response management ?

- Policies, training, logs, plans, for effective reporting of attack events.

Why is incident report management important?

- Effective incident response management is needed to quickly respond recover or quarantine an attack.

CIS Control 18: Penetration testing

- What is penetration testing ?
  - Testing the fortification of Enterprises assets by means of ethical hacking.
- Why is penetration testing important ?
  - Penetration testing helps cyber security defenders discover vulnerabilities in an Enterprise cyber network.

References

- https://www.cisecurity.org/controls/v8/
- https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
- https://www.oceg.org/standards/
- https://compliancy-group.com/hipaa-rules-and-regulations/
- https://www.youtube.com/watch?v=q2t91jLmh3k – Penetration testing