LECTURE 2
COMPUTER SECURITY OPERATION

Computer Operation Security

- Act of understanding the threats to and vulnerabilities of computer operations in order to routinely support operational activities that enable computer systems to function correctly
- Operation security associated with everything that takes place to keep a network, computer system, application and environment up and running securely.
- Includes maintenance of an environment and activities that should take place on day to day basis
- Operational security – high priority to ensure security of information and Information Technology asset under organization control

Computer Operation Security

- *Domain is concerned*:
  - Threats, Vulnerabilities and Assets
  - Threats to operation security can be defined as the presence of any potential event that could cause harm by violating security. Example – operator's abuse of privileges that violates confidentiality – simple e.g.: *Selling PMR examination sheets*
  - Vulnerabilities; weakness in a system that enables security to be violated. Example weak implementation of separations of duties
  - Assets – anything – computing resources and ability **i.e., hardware, software, data and personnel**.

Topics

- **Asset Management**
- Common Security Control
- Monitoring and Audit
- Threats and Vulnerabilities
- Security Awareness & Training

Asset Management

- Asset management is intended to first identify all hardware, software, systems, and data that support a facility's information systems.
- Once that baseline is completed, regular audits and assessments should be conducted periodically (e.g., on an annual or biannual basis).
- This is to ensure that the system is operating as designed and approved.

Asset Management

Asset Management Security Control

- Activity/Security Control:

Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the facility's network.

- Rationale:

An asset inventory is critical as the facility cannot protect unidentified assets.

Asset Management

Asset Management Security Control

- Activity/Security Control:

Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to a facility's public and private network(s).

- Rationale:

A facility cannot protect systems it does not know it has. An automated tool can identify assets that might have been missed following a traditional inventory process.

Asset Management

Asset Management Security Control

- Activity/Security Control:

Deploy dynamic host configuration protocol (DHCP) server logging.

- Rationale:

It is important to be able to detect unknown devices that may try to connect to a facility's information system. DHCP server logging can help accomplish this objective.

Topics

- ~~Asset Management~~
- **Common Security Control**
- Monitoring and Audit
- Threats and Vulnerabilities
- Security Awareness training

Common Security Control

I. Access Control
II. Baseline Configuration Security
III. Communications Security
IV. Cryptography
V. Information Sanitization and Destruction
VI. Human Resource Security
VII. Operational Security
VIII. Physical and Environmental Security
IX. Security in Supplier and Third-Party Relations
X. Security throughout the Asset Life Cycle

Asset Management

Common Security Control (Access Control)

- Access control is designed to ensure that someone without permission to access an information asset, or without a need to know that information, is restricted from access.
- Access can take many forms, such as digital or physical access to an information system or physical access to an information repository.
- Examples of digital access include accessing an information system using the facility's onsite network, remote access from an external site (e.g., a parent facility's computer network, a remote access location), and website access.
- In all cases, access to an information system must be granted, disabled, or revoked using an approved and documented process.
- Access credentials should never be shared, unless permission has been granted based on operational considerations and the security risks involved are explicitly accepted by the facility.

Asset Management

Common Security Control (Baseline Configuration Security)

- Establishing a configuration to which all systems need to adhere is important for maintaining a safe and secure information infrastructure.
- This configuration is referred to as the baseline, meaning all systems shall at a minimum implement the security controls needed to maintain that baseline.
- Facilities shall establish and maintain baseline configurations systems (including hardware, software, firmware, and documentation) throughout the system's life cycles; and as well as establish and enforce security configuration settings for all systems.
- The baseline must be assigned to, and owned by, an individual or group within the facility who has the authority granted by management to establish, review, update, and maintain the baseline.

Asset Management

Common Security Control (Communications Security)

- Protection of digital communications is important because anyone with malicious intent and access to the network can “sniff” or eavesdrop on facility communications.
- These protections are also important in preventing the unintentional leak of the facility’s sensitive information to groups that do not need this information, and more importantly can prevent information from leaking outside of the facility.
- These communication security controls are typically implemented in the facility’s firewalls, web proxy, and intrusion detection system/intrusion protection system (IDS/IPS).
- The rules and policies should be reviewed regularly, at least annually, to ensure that rules are still needed, and that new rules do not cancel out old rules.

Topics

- ~~Asset Management~~
- ~~Common Security Control~~
- **Monitoring and Audit**
- Threats and Vulnerabilities
- Security Awareness training

Monitoring & Audit

- Security controls are deployed with the intent of deterring, delaying, detecting, or denying an attack.
- Monitoring and auditing security controls address the detection element of security.
- Security personnel must continuously acquire, assess, and take action on new information in order to identify and mitigate vulnerabilities and minimize the window of opportunity for attackers.
- Automated tools for monitoring and auditing can be implemented at an affordable cost and can substantially increase the facility's ability to assess the security status of its information systems.

Monitoring & Audit

- These software tools can provide a security trend analysis and to proactively protect against emerging threats.
- A robust information security program will include capabilities for the collection and analysis of indication and warning data to detect and respond to intrusions.
- These data can come from many different devices and applications in a networked environment.
- Common examples include event and logging information originating from routers, firewalls, proxies, operating system security event logs, and application logs.

Activity / Security Control	Rationale
Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system.	Allowing only authorized software limits the attack surface of a facility.
Closely monitor and/or block dangerous file types (e.g., .exe, .zip, .msi).	Preventing known dangerous file types reduces the attack surface.
Run automated vulnerability scanning tools against all systems on an information security system. Perform these scans on a weekly or more frequent basis. Deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator.	Vulnerability scanners help identify both code-based vulnerabilities (such as those described by common vulnerabilities and exposures entries) and configuration-based vulnerabilities.

Topics

- ~~Asset Management~~
- ~~Common Security Control~~
- ~~Monitoring and Audit~~
- **Threats and Vulnerabilities**
- Security Awareness training

Threat & Vulnerabilities

Cyber Threats + Vulnerabilities

Attacks/Incidents

Threat

What is a Cyber Threat?

"the possibility of a malicious attempt to damage or disrupt a computer network or system"

This definition is incomplete without including the attempt to access files and infiltrate or steal data.

“the threat is more closely identified with the adversary attempting to gain access to a system”

OR

“threat might be identified by the damage being done, what is being stolen or the Tactics, Techniques and Procedures (TTP) being used”

The Most Common Cyber Threat?

1. Social Engineered Trojans
2. Unpatched Software (such as Java, Adobe Reader, Flash)
3. Phishing
4. Network traveling worms
5. Advanced Persistent Threats

Furthermore, two technology trends that are driving the cyber threat landscape nowadays are:

- Internet of things – individual devices connecting to internet or other networks
- Explosion of data – stored in devices, desktops and elsewhere

The Most Common Cyber Threat?

Today, the list of cyber threats may look more like this, and cyber threats are typically composed of a combination of these:

- Advanced Persistent Threats
- Phishing
- Trojans
- Botnets
- Ransomware
- Distributed Denial of Service (DDoS)
- Wiper Attacks
- Intellectual Property Theft
- Theft of Money
- Data Manipulation
- Data Destruction
- Spyware/Malware
- Man in the Middle (MITM)
- Drive-By Downloads
- Malvertising
- Rogue Software
- Unpatched Software

Most Common Sources of Cyber Threats

- Nation states or national governments
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists and hackers
- Business competitors
- Disgruntled insiders

Best Practices for Defense and Protection

- Today's best practices for cyber security are a hybrid approach. Keeping up with rapid advancements in cyber threats roles that go beyond what is feasible for an in house security team to provide.

- **Security Partner Efforts:**
  1. Penetration testing and vulnerability scanning
  2. Advanced threat monitoring of endpoints
  3. Always up to date threat intelligence
  4. Emergency incident response staff and investigators on call

*If resources are not available in-house, any of these efforts can be pushed to a managed security services provider.

Best Practices for Defense and Protection

- **In-House IT Security Efforts:**

Strong end user education – compliance based practices for handling data, recognizing phishing attempts and procedures to counteract human engineering attempts.

1. Up to date software
2. Firewall and anti-virus*
3. IDS/IPS* – intrusion detection systems and intrusion prevention systems
4. Security event monitoring*
5. Incident response plan*

Best Practices for Defense and Protection

- **Apply Common Sense:**
  1. Keep your software updated
     *Keep your antivirus and malware detection software up-to-date
  2. Do not reuse passwords
  3. Use strong passwords
  4. In case of developing software, sanitize inputs
  5. Do not run unnecessary services

Vulnerabilities

"a weakness of an asset or control that can be exploited by one or more threats"

Technical Vulnerability

- Operating systems and applications have been developed from millions of lines of complex code and often have a variety of errors and oversights that are left in the system once compiled.
- These errors are not necessarily ones that affect operations therefore are not found until someone specifically tries to find ways to exploit your systems.
- When security researchers discover vulnerabilities, vendors are usually given a relatively short period of time to create a patch before the researchers notify the public about the problem.

Vulnerabilities

Technical Vulnerability

- A bug might be found in a shared cryptographic function that has been compiled into dozens if not hundreds of end user application, and in each case the vendor will need to wait for the cryptographic function to first be patched, and then recompile their own software and release a patch of their own.

Non-Technical Vulnerability

- As a security manager you need to properly understand how ***physical and process vulnerabilities*** affect your business and security and how they should be addressed within a holistic approach to your security architecture.

Vulnerabilities

Non-Technical Vulnerability

physical vulnerabilities

- Any threat in the electronic world, they still need to exploit a vulnerability or weakness to have any kind of negative effect on our systems or information.
- The sorts of areas that need to consider, where non-technical vulnerabilities will affect the organization are premises security, access control and general staff awareness.

process vulnerabilities

- The technical vulnerabilities in systems are just one perspective of where you'll find weaknesses that can affect a loss of confidentiality, integrity, or availability.
- Security managers need to be aware of the underlying processes that keep the business safe and ensure that there are minimal vulnerabilities in those that can also lead to a compromise

Vulnerabilities

Non-Technical Vulnerability

process vulnerabilities

- For example, a process may be dictate that the keys to the server racks in the data center are held by the security guard and an engineer needing access needs to seek written permission from the security manager, which needs presenting to the guards prior to keys being issued.

- However, if an attacker knows what the form looks like and has found a way to forge the security manager's signature, if this form is all the attacker needs to get the keys to the server room, then gaining malicious access will be easy.

Topics

- ~~Asset Management~~
- ~~Common Security Control~~
- ~~Monitoring and Audit~~
- ~~Threats and Vulnerabilities~~
- **Security Awareness training**

Security Awareness & Training

- The purpose of security awareness and training is to provide personnel facility with the skills needed to minimize information security risks.
- This begins by assessing the current level of information security knowledge in order to identify knowledge gaps between what personnel know and put into practice, and what the facility is targeting for information security practices.
- Knowledge of gaps is used to enhance the design of information security training.
- Many facilities find it appropriate and efficient to incorporate information security with cyber security and physical security training because so many elements are common to all three security topics

Security Awareness & Training

- Information security training is needed for all functional roles in the facility for general personnel, information system and sensitive information users and program managers, and information security specialists.
- The amount of training required varies for the different functional roles.
- Training also should be provided to vendors, contractors, corporate staff, and regulators who have a legitimate need to access the facility's information systems or sensitive information.

Roadmap/Mind Map