Implementing Policies to Mitigate Risk

Objectives:

- Use the appropriate tools to assess the security posture of an organization

- Troubleshoot common security issues

- Differentiate common account management practices

- Policy Plans for an Org

- Incident Response Procedures

- Basic Concepts of Forensics

Exploring Security Policies

- Security Policies are documents that lay out a security plan in a company
  - These are administrative controls used to reduce and manage risks
    - The end result is that when Policies are enforced they help prevent incidents, data loss and theft.
      - Companies develop (SOPs) Standard Operating Procedures to support security policies

Onboarding

- Onboarding is the process of granting individuals' access to organizations computing resources. The employee is provided with a user account and computer.
  - Offboarding is the opposite of onboarding, which would be the process of revoking access which is done after the interview
    - Users must also delete email company email accounts from their mobile devices or their devices are subject to being wiped clean

Personnel Management Policies

- ALL COMPANIES HAVE THESE TO DEFINE ISSUES RELATED TO PERSONNEL MANAGEMENT
  - Some of these policies are directly related to Security. These are:
    - Acceptable Use
    - Mandatory Vacations
    - Separation of Duties
    - Job Rotation
    - Clean Desk Policies

Implementing Policies to Mitigate Risk

Acceptable Use Policy

- Acceptable Use Policy (AUP) defines proper system usage or the rules of behavior for employees when using information technology (IT) systems.
    - This describes the purpose of computer systems and networks, how users can access them, and the responsibilities of users when they access these systems.
        - Many organizations monitor employee activities, such as web sites they visit and what data they send out by email.
            - The AUP often includes definitions of unacceptable use. For example employees may be prohibited from accessing social media sites

Mandatory Vacations

- Mandatory vacation policies help detect when employees are involved in malicious activity such as fraud or embezzlement.
    - As an example employees that are in a position of fiscal trust such as stock traders or bank employees are required to take an annual vacation of at least 5 consecutive workdays.
        - For embezzlement actions of any substantial size to succeed, the employee would need to be constantly present to manipulate records.
            - If the employee is gone on vacation someone else would have to be responding to queries during the employees absence and this can lead to discovering illegal activities.
                - This is not only used in the financial industry. In many companies outside of the financial industry, system administrators are also required to take vacations to make sure they are not doing anything illegal

Separation of Duties

- Separation of Duties is the principle that prevents any single person or entity from being able to complete all the functions of a critical or sensitive process. It’s designed to prevent fraud, theft or errors.
- An example is dividing sensitive tasks up so it is not just one person who signs checks.
    - Lets, say an accounting department is split into accounts receivable and accounts payable.
    - If Homer were the only person doing all these functions it would be possible for him to create and approve a bill from Homer’s most excellent Retirement Account and after approving the bill, Homer would then pay it.
        - In another example a group of IT administrators may be assigned to maintain database servers. They would not be granted access to security logs. Instead security admins will have access to the security logs, but the security administrators would not have access to data within the Databases.will have access to the security logs, but the security administrators would not have access to data within the Databases.

Implementing Policies to Mitigate Risk

Job Rotation

- Job rotation is the concept employees rotate through different jobs to learn the processes and procedures in each job.
- From a security perspective, job rotation helps prevent or expose dangerous shortcuts or even fraudulent activity.
    - Imagine a single person always performs the same function without any escalation or oversight. This increases the temptation to go outside the boundaries of established policies
    - Job rotation policies work well together with separation of duties policies.
        - A separation of duties policy works well however, two people together can still collude to defraud the company.
        - If a job rotation policy is included, these two people will not be able to continue fraudulent activity indefinitely

Clean Desk Policy

- A clean desk policy directs users to keep their areas organized and free of papers.
- This helps prevent the possibility of data theft or inadvertent disclosure of information.
    - Imagine you go to a bank to meet with a load officer in their office.
    - The load officer has stacks of information on their desk, including loan applications from many customers.
        - If the load officer steps out of the office, the attacker can either grab some documents or start taking pictures with a mobile device.

Background Check

- It’s common to perform background checks on potential employees, even after they are hired.
    - A background check will vary based on responsibilities and the nature of the job, however all employees are subject to background checks no matter what the job.
    - Many organizations also check a person's financial history.
        - It is also common to check a person's online activity. This includes checking activity on social media sites.
        - Example of Year Up Intern and picture on Facebook

NDA (Non Disclosure Agreement)

- This is an agreement that is signed by two entities to keep proprietary data confidential and not disclose it to outside entities.
    - Many organizations use an NDA to prohibit employees to share information not only when employed but also after they leave a company.

Implementing Policies to Mitigate Risk

Exit Interview

- An exit interview is conducted with employees before they leave an organization. This is done for employees who leave voluntarily and those who are laid off or fired.
- The overall purpose is for the employer to gain information from departing employees.
    - **Some potential questions are:**
    - What did you like most/ or least about your job here.
    - Do you think you had adequate training to do your job
    - Why did you leave your current position
    - What is the working relationship you had with your manager
    - What skills and qualifications does your replacement need to excel in this position
        - After the interview all company equipment is collected and the person's account is disabled

Policy Violations & Adverse Actions

- The action depends on the severity.
- Let's say an employee sends out an email to the entire company inviting them to their church. The person's manager may choose to verbally counsel them against this and a note will be placed in the person's HR folder.
    - If an employee starts a cyber bullying campaign against another employee in the company, they are likely to be fired immediately with no warnings.

Other General Policies

- An organization may implement personnel management policies that affect other areas of an employees life. Some examples include employee actions on social media sites and email.
- Employees cannot post derogatory comments about fellow employees or customers or else they will be fired.
    - Here’s an example: In June of 2020, FedEx employee fired, NJ corrections officer suspended over video mocking George Floyd.

Social Media Networks & Applications

- Social Media sites present risks to companies by employees inadvertently posting confidential information.
    - Attackers use social media sites to gather personal information about people who work for companies they want to attack.
    - People often post their favorite books, dates of graduation, high school they went to and other information on Facebook.
        - This is the type of challenge questions that may be asked of a person seeking to change their password on a site.

Implementing Policies to Mitigate Risk

Examples of Information Taken From Social Media Sites

- David Kernell used Yahoo’s cognitive password account recovery process to change former Alaska’s governor Sara Palin’s password for her email account. At the time Yahoo asked questions like your birthdate and high school in order to change your password.
    - This didn’t work out well for David Kernell. He was convicted of a felony and spent over a year in jail
        - While vacationing in Paris Kim Kardashian was regularly posting her status and location on social media. She also stressed she did not wear fake jewelry.
            - Thieves robbed her at gunpoint in her Paris hotel room. She was bound and aged and a ring worth $4.9 million was stolen plus more jewelry worth 5.8 million.
                - When caught one of the thieves said it was easy to track her through her online activity.

Banner Ad Malvertisements

- Attackers have been delivering malware through banner ads for several years now.
    - Many of these attacks redirect users to another site where malware is installed. These ads used to use flash but flash is now disables on most sites now because of its use by hackers delivering malware.
        - These include sites advertising fake antivirus software. When you clicked on a link to get this antivirus software, you got a virus

Implementing Policies to Mitigate Risk

Protecting Data

- Data policies assist in the protection of data.
    - This section will point out the elements that may be contained in data policy.

Information Classification

- Organizations identify, classify and label data they use.
    - Here are types of data:
    - **Public Data** – available to anyone
    - **Confidential Data**- information company intends to keep secret among a slect group of people. For example most companies keep salary data confidential. Only people in the accounting dept and some executives would know this, most companies prohibit employees from sharing their salary information
    - **Private Data** – this is information about an individual that should remain private. This comes under PII (Personal Identifiable Information. There is also PHI which is Personal Health Information.

Data Destruction and Media Sanitation

- When computers reach end of life companies dispose of them in some way. There needs to be company policy that makes sure these computers do not contain ANY data.
- It's common for an organization to have a checklist to make sure the computers are **sanitized** before a company disposes of them.
    - **Data destruction** includes hard drives and paper.
        - **Purging**- is a general sanitization term indicating all sensitive data has been removed from a device.
        - **File Shredding** – Al l remnants of a file are removed. This is done by repeatedly overwriting a space on a drive. With 1s and 0s; In some cases, hard drives are actually shredded by a machine
            - **Wiping** – Drives that are wiped use a disk wiping tool that wipes one bit at a time. This makes data on a disk unreadable.
            - **Erasing** – Solid state drives cannot be wiped by conventional methods. They must be destroyed.
            - **Burning**- Many organizations burn printed materials in an incinerator.

Data Retention Policies

- **A data retention policy identifies how long data must be retained**, sometimes specifying what type of device to store the data on.
    - This reduces the amount of resources needed to store the data.

        - Data retention policies also meet legal requirements. Some laws mandate the retention of data for a certain amount of time. For example insurance companies must retain data for seven years.

PII & PHI

- Some Examples are:
- Full name
- Birthday and birthplace
- Medical and Health information
- Street and email address
- Biometric data
- Any type of identification number like SSN

In general you need two or more pieces of information to make it PI.

Protecting PII & PHI

- Organizations have an obligation to protect PII
- There are many laws that mandate the protection of PII
- There are legal and Compliance issues in keeping this information private
    - Refer to slides with Compliance Issues

Data Roles & Responsibilities

- Many people in an organization handle data. These people have specified roles
- **Owner**- The data owner is the person with overall responsibility for the data. It is often a high level position like the CEO or CIO.
- **Steward/Custodian** – This person handles routine tasks to protect the data. For example the data custodian would ensure data is backed up on a regular basis. They would also ensure everything is properly labeled. The data owner would typically delegate this task to the data custodian
- **Privacy Officer**- This person is responsible for ensuring the organization is complying with relevant laws such as HIPPA SOX etc…

Responding To Incidents

- Many organizations have incidence response procedures.
- Incidents could be release of malware, security policy violations, unauthorized access of data and in appropriate use of systems.
    - Organizations regularly review and update security policy
    - One example from the early days of computer systems was when a hacker broke into a government computer system and the first thing he saw was a welcome message. He started poking around but was caught and arrested. In court he told the judge that when he broke in he saw the welcome message and thought he was being invited to look around. The welcome message prevented the

government organization from taking legal action against the hacker. **You will no longer see welcome banners on company and government computers**.

Incident Response Plan

- This provides details on how to respond to an incident
    - **Definition of Incident Types**- This section helps employees distinguish between something that might not be a security incident and something that is. Some incidents include attacks from botnets, malware, delivered by email, data breach, ransom etc.…
    - The plan may group specific incident types together.
        - **Cyber Incident Response Teams**- a cyber incident response team is composed of employees with expertise in different areas. Combined they have the knowledge and experience to respond to many types of incidents The team has extensive training.
        - **Roles and Responsibilities-** Often roles for an incident response team are specified For example a team might not only include people in technical roles but also someone in upper management with the authority to get things done.
        - **Escalation**- After identifying an incident, it has to be escalated. Escalation could be for a technician to inform their manager that they discovered malware. If a critical server is involved in a Ddos attack, all members of the incident response team may be required to be involved.
            - **Reporting**- requirements Depending on the severity, security personnel may have to inform executives in the company of the incident. For example if customer data has been compromised an incident report must be delivered to senior management exercises One method of preparing for an incident response is to perform exercises.
            - **For example** a technical exercise may include a test of the admins ability to rebuild a server after a simulated attack. The plan specifies who should be notified and when.

Incident Response Process

- Incident Response contains multiple phases. Some common phases which are:
- **Preparation** – This phase occurs before the incident and specifies how personnel should respond to the incident. It includes a plan and procedures.
- **Identification** – Time is taken to verify this is an actual incident and not a false positive or false alarm
- **Containment** – after an incident occurs, personnel attempt to contain it and isolate it. This can be as simple as unplugging the network interface card to disconnect the systems from the internet. Or you can modify access control lists or a firewall. The goal here is to prevent the attack from spreading to other computers on the network

Implementing Policies to Mitigate Risk

- **Eradication** – After the attack is contained, it is often necessary to remove infected components from the network.

It is important for example to remove all the malware that is on the network.

Incident Response Process (continued)

- **Recovery-** During recovery all affected systems are restored to normal operation. Before they are reconnected to the network it must be confirmed they are operating normally. This may include rebuilding systems from images, restoring from backups and installing updates. All vulnerabilities that have been identified to cause the incident must be removed.
- **Lessons Learned** – After the incident is handled the security team performs a lessons learned review. This may result in a modification or procedures

Implementing Forensic Procedures

- A forensic evaluation helps the organization collect and analyze data as evidence it can use in the prosecution of a crime. The evidence must be handled with the assumption it will be used as evidence in court
  - Because of these forensic practices protect evidence to prevent modification and control evidence after collecting it.
    - The procedures are the same as forensic evidence collected from crime scenes
      - Kali linux includes a wide variety of forensic tools

Order of Volatility

- This refers to the order in which you should collect evidence.
  - Volatile refers to evidence that is not permanent. You should collect evidence that is most volatile first. RAM is the most volatile. It disappears as soon as you power down a computer. Because of this you should never power down a computer during an incident or you may destroy important evidence. There are many tools designed to capture volatile data. Once the data is captured you can power down the computer.
    - Data in cache memory= processor and hard drive cache
    - Data in Ram- system and network processes
    - A PAGING FILE OR SWAP FILE ON THE SYSTEM DISK DRIVE
    - Data stored on local disk drives
    - Logs stored on remote systems
    - Archive media
      - The security book explains in detail the preservation of evidence but too deep and detailed for here.

Chain of Custody

Implementing Policies to Mitigate Risk

A chain of custody is a process that provides assurances that evidence has been controlled and handled properly after collection

- Forensic experts always establish a chain of custody.
- Everything must be documented and tagged