Laboratory #4

Lab 4: Craft a Layered Security Management Policy – Separation of Duties

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify roles and responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure
- Identify physical separation of duties regarding responsibility for information systems security policy implementation
- Align responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure
- Apply separation of duties to a layered security management policy throughout the seven domains of a typical IT infrastructure
- Create a layered security management policy defining separation of duties

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #4:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #4 – Student Steps

The following steps are required to conduct this lab:

1. Review the seven domains of a typical IT infrastructure diagram, as shown in Figure 1
2. Discuss what the roles, responsibilities, and accountabilities are throughout the seven domains of a typical IT infrastructure regarding information systems security

3. Discuss how these roles, responsibilities, and accountabilities are crucial to define who is responsible for what throughout the IT infrastructure
4. Discuss the importance of separation of duties and how involving key personnel for a security incident response team is important
   - Separation of duties
   - No one individual should have too much authority or power to perform a function within a business or organization
   - Understanding one's domain of responsibilities and where that responsibility stops is critical to understand separation of duties
5. Review the deliverables needed for Lab 4: Create a Layered Security Management Policy - Separation of Duties
6. Review the Policy Definition Template they are to use for the creation of the Separation of Duties Policy Definition for a layered security management plan for an IT Infrastructure

Deliverables

Upon completion of Lab #4 – Craft a Layered Security Management Policy - Separation of Duties, the students are required to provide the following deliverables as part of this lab:

1. Lab #4 – Policy Definition for a Layered Security Management Plan – Separation of Duties
2. Lab #4 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #4 that the student must perform:

1. Was the student able to identify the roles and responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to identify the physical separation of duties regarding responsibility for information systems security policy implementation? – [**20%**]
3. Was the student able to align responsibilities for policy implementation throughout the seven domains of a typical IT infrastructure? – [**20%**]
4. Was the student able to apply separation of duties to a layered security management policy throughout the seven domains of a typical IT infrastructure? – [**20%**]
5. Was the student able to create a layered security management policy defining separation of duties? – [**20%**]

Lab #4 – Assessment Worksheet

Craft a Layered Security Management Policy – Separation of Duties

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: _____

Lab Due Date: 12/10/2024

Overview

In this lab, you are to create a security management policy that addresses the management and the separation of duties throughout the seven domains of a typical IT infrastructure. You are to define what the information systems security responsibility is for each of the seven domains of a typical IT infrastructure. From this definition, you must incorporate your definition for the separation of duties within the procedures section of your policy definition template. Your scenario is the same as in Lab #1 – ABC Credit Union/Bank.

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and the use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation of the organization.
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees.
- The organization wants to monitor and control use of the Internet by implementing content filtering.
- The organization wants to eliminate personal use of organization owned IT assets and systems.
- The organization wants to monitor and control the use of the e-mail system by implementing e-mail security controls.
- The organization wants to implement this policy for all IT assets owned by the organization and to incorporate this policy review into the annual security awareness training.
- The organization wants to define a policy framework including a Security Management Policy defining the separation of duties for information systems security.

Instructions

Using Microsoft Word, craft a Security Management Policy with Defined Separation of Duties using the following policy template:

ABC Credit Union

Policy Name

Policy Statement

{Insert policy verbiage here}

This policy establishes security management practices with clear separation of duties across all seven domains of ABC Credit Union/Bank's IT infrastructure, aiming to protect organizational data and systems.

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

The policy aims to prevent insider threats and errors, ensure compliance with GLBA, and secure organizational assets by defining roles and responsibilities in each domain.

Scope

{Define whom this policy covers and its scope.

Which of the seven domains of a typical IT infrastructure are impacted? – All 7 Must Be Included in the Scope.

What elements or IT assets or organization-owned assets are within the scope of this policy? – In this case you are concerned about what IT assets and elements are within each of the domains that require information systems security management?}

Applies to all employees, contractors, and third-party providers with access to IT assets across all seven domains: Workstation, LAN, WAN, Perimeter, Remote Access, Server, and User Domains.

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards – Yes, you need to reference technical hardware, software, and configuration standards for IT assets throughout the seven domains of a typical IT infrastructure. For this lab, you can merely point them to "Workstation Configuration Standards", etc.}

References security standards like Workstation Configuration Standards, Network Configuration Standards, and Server Security Standards for implementing security across IT domains.

Procedures

{Explain how you intend to implement this policy for the entire organization. This is the most important part of the policy definition because you must explain and define your separation of duties throughout the seven domains of a typical IT infrastructure. All seven domains must be listed in this section as well as who is responsible for ensuring C-I-A and security policy implementation within that domain.}

Defines separation of duties within each domain, ensuring that responsibilities like system configuration, access control, and monitoring are clearly assigned to prevent unauthorized access and maintain data security.

Guidelines

{Explain any road blocks or implementation issues that you must overcome in this section and how you will surmount them per defined policy guidelines. Any disputes or gaps in the definition and separation of duties responsibility may need to be addressed in this section.}

Highlights challenges such as employee resistance, role confusion, legacy system issues, and inter-departmental coordination, with strategies to overcome them through training, clear documentation, and regular communication.

Note: Your policy document must be no more than 3 pages.

Lab #4 – Assessment Worksheet

Craft a Layered Security Management Policy – Separation of Duties

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name:

Lab Due Date: 12/10/2024

Overview

In this lab, you examined the seven domains of a typical IT infrastructure from an information systems security responsibility perspective. What are the roles and responsibilities performed by the IT professional, and what are the roles and responsibilities of the information systems security practitioner? This lab presented an overview of exactly what those roles and responsibilities are and, more importantly, how to define a security management policy that aligns and defines who is responsible for what. This is critical during a security incident that requires immediate attention by the security incident response team.

Lab Assessment Questions & Answers

1. For each of the seven domains of a typical IT infrastructure, summarize what the information systems security responsibilities are within that domain:
   + Workstation Domain:Ensure secure configurations, monitor activity, enforce usage policies, and implement content and email security.
   + LAN Domain:Protect internal network, control access to data, and ensure data integrity through firewalls and segmentation.
   + WAN Domain:Secure external communications with encryption, monitor traffic, and control unauthorized access.
   + Perimeter Domain:Protect organizational boundaries using firewalls, intrusion prevention, and secure access techniques.
   + Remote Access Domain:Secure remote connections with VPNs and multi-factor authentication, and monitor remote access logs.
   + Server Domain:Apply security patches, manage access, and monitor server logs for unusual activity.
   + User Domain:Implement strong authentication, conduct security training, and perform regular audits for compliance.

2. Which of the seven domains of a typical IT infrastructure requires personnel and executive management support outside of the IT or information systems security organizations?

The User Domain requires personnel and executive management support outside of the IT or information systems security organizations

3. What does separation of duties mean?

Separation of duties (SoD) is a security principle that ensures no single individual has control over all aspects of any critical function or process. This is done to prevent fraud, errors, and misuse of power within an organization

4. How does separation of duties throughout an IT infrastructure mitigate risk for an organization?

Separation of duties (SoD) in an IT infrastructure mitigates risks for an organization by ensuring that no single individual has complete control over critical processes or systems. This division of responsibilities helps prevent a range of risks such as fraud, errors, and security breaches. Here's how SoD mitigates risks:
+ Prevents Fraud and Malicious Activities
+ Reduces Errors and Mistakes
+ Improves Accountability
+ Limits Access to Sensitive Information
+ Helps in Compliance and Auditing
+ Minimizes Insider Threats
+ Enhances Incident Detection and Response

5. How would you position a layered security approach with a layered security management approach for an IT infrastructure?

+ A layered security approach (defense in depth) applies multiple security layers (e.g., perimeter, network, endpoint, application, data, and user security) to protect IT infrastructure, ensuring that if one layer is breached, others provide continued protection.
+ A layered security management approach focuses on the effective management of these security layers through policies, monitoring, incident response, risk management, compliance, and continuous improvement.
+ How they complement each other:
  - Layered security deals with the technologies and tools used at each security layer.
  - Security management ensures these layers are implemented, monitored, and maintained effectively with proper governance, training, and incident response.Both approaches work together to create a resilient and adaptive security posture

6. If a system administrator had both the ID and password to a system, would that be a problem?

Yes, it would be a problem. If a system administrator has both the ID and password to a system, it could create a significant security risk. Here's reason:
+ Lack of Separation of Duties: One of the key principles in information security is separation of duties. This ensures that no single individual has full control or access to all parts of a system or process. Allowing a system administrator to have both the ID and password violates this principle and increases the risk of misuse or errors.
+ Increased Risk of Insider Threats: If a system administrator has access to both the credentials and the ability to perform system administration tasks, they could potentially misuse their access for malicious purposes, either intentionally or accidentally.
+ Accountability Issues: When a system administrator has full access with both ID and password, it can be difficult to track who is responsible for specific actions in the system. If something goes wrong, it's harder to identify the source of the problem or assign accountability.
+ Compromise Risk: If the system administrator's credentials are compromised, an attacker would have complete control of the system, making it easier to carry out malicious activities

7. When using a layered security approaches to system administration, who would have the highest access privileges?

In a layered security approach to system administration, the highest access privileges are typically held by:
+ Root/Superuser: Has unrestricted access to all system components, often used for critical tasks.
+ System Administrator: Manages the operating system, software, and user permissions, with broad control but within defined roles.
+ Network Administrator: Manages network infrastructure, such as routers and firewalls, with network-focused access.
+ Application/Database Administrators: Manage specific areas like databases or applications, with powerful access within their domain.
+ Security Administrators: Oversee security measures like firewalls and monitoring, but usually not full control of the entire system.

8. Who would review the organizations layered approach to security?

The review of an organization's layered security approach is typically done by:
- CISO: Oversees the overall security strategy.
- IT Security Team: Monitors and implements security measures.
- Executive Management: Ensures security aligns with business objectives.
- Audit Team: Conducts independent security assessments.
- Compliance Officers: Ensures adherence to legal and regulatory requirements.
- Risk Management Team: Evaluates risk mitigation.
- Penetration Testers/Red Teams: Test for vulnerabilities through simulated attacks.

9. Why do you only want to refer to technical standards in a policy definition document?

- Consistency: Technical standards provide clear, universally accepted benchmarks that help ensure consistency in security practices across all systems and domains.
- Clarity: They define specific requirements for configurations, hardware, and software, making it easier for employees to follow and implement security measures accurately.
- Compliance: Many technical standards are aligned with legal, regulatory, or industry best practices, ensuring that the organization remains compliant with security requirements.
- Scalability: As organizations grow, technical standards help maintain a cohesive and scalable approach to security, simplifying management and integration of new systems.
- Minimizes Errors: Technical standards reduce the risk of errors or misconfigurations that could lead to vulnerabilities or breaches.
- Efficiency: They streamline the process of policy implementation by providing clear guidelines on how systems should be secured, reducing the need for repetitive decisions.

10. Why is it important to define guidelines in this layered security management policy?

- Clarifies Expectations: Guidelines help clarify how security policies and procedures should be implemented, making it easier for employees to understand their roles and responsibilities in maintaining security.
- Mitigates Implementation Challenges: Security guidelines provide practical steps and best practices, addressing potential roadblocks, and ensuring smooth implementation of security measures across the organization.
- Adapts to Different Scenarios: Guidelines allow for flexibility in how policies are applied in different situations or departments, ensuring the security framework can adapt to specific needs or challenges.
- Ensures Compliance: By setting clear rules and best practices, guidelines help ensure that the organization remains compliant with internal policies and external regulations.
- Addresses Gaps or Disputes: If there are disputes or gaps in the separation of duties or other policy areas, guidelines can offer direction on resolving them, ensuring consistency in decision-making.
- Enhances Security Awareness: Providing guidelines reinforces the importance of security at every level, encouraging employees to be proactive in identifying and addressing risks.

11. Why is it important to define access control policies that limit or prevent exposing customer privacy data to employees?

- Protecting Customer Privacy: Customer privacy data, such as personal information and financial details, is highly sensitive. Limiting access ensures that only authorized personnel can view or handle this information, reducing the risk of misuse or unauthorized access.
- Compliance with Regulations: Many countries have strict data protection laws, such as GDPR (General Data Protection Regulation) or CCPA (California Consumer Privacy Act), which mandate that organizations safeguard customer data. Access control policies ensure compliance with these legal requirements, helping to avoid penalties or legal actions.
- Reducing Insider Threats: Not all employees need access to customer data for their roles. Limiting access reduces the chances of malicious actions, such as data theft or data leakage, by employees who may have ill intent.
- Minimizing Human Error: By restricting access to sensitive data, organizations can prevent unintentional mistakes, such as accidental data sharing or mismanagement, which could compromise customer information.

12. Explain why the seven domains of a typical IT infrastructure helps organizations align to separation of duties.

The seven domains of a typical IT infrastructure help organizations implement separation of duties by clearly defining roles and responsibilities across different areas, reducing risks like insider threats, system misconfigurations, or unauthorized access.
- User Domain: Ensures distinct roles for users, preventing conflicts of interest in accessing sensitive systems.
- Workstation Domain: Separates responsibilities for workstation management and security.
- LAN Domain: Differentiates between network maintenance and data management tasks.
- WAN Domain: Segregates external connection monitoring from internal system management.
- System/Application Domain: Ensures separate teams for development, testing, and production, preventing unauthorized system changes.
- Security Domain: Distinguishes between security monitoring and infrastructure management roles.
- Data Domain: Separates data management tasks from backup and recovery responsibilities

13. Why is it important for an organization to have a policy definition for Business Continuity and Disaster Recovery?

- Minimizes Downtime: BC and DR policies ensure that in the event of a disaster (e.g., system failure, cyberattack, natural disaster), the organization can quickly resume critical business operations with minimal disruption.
- Risk Management: These policies identify potential risks and outline procedures to mitigate the impact of disruptions, protecting the organization from financial, reputational, and operational damage.
- Compliance: Many industries require organizations to have documented BC and DR plans to comply with regulations or standards like ISO 22301 or HIPAA, ensuring that business processes are maintained in emergencies.
- Data Protection: DR policies specifically safeguard important data and ensure that systems are backed up, reducing the risk of data loss.
- Employee and Stakeholder Confidence: Having a well-defined BC and DR plan instills confidence in employees, customers, and stakeholders, showing the organization is prepared to handle unexpected disruptions.
- Efficient Resource Allocation: A policy helps allocate resources and responsibilities clearly, making the recovery process more organized and efficient during an emergency

14. Why is it important to prevent users from downloading and installing applications on organization owned laptops and desktop computers?

- Security Risks: Unapproved or unauthorized applications may contain malware, ransomware, or other malicious software that can compromise the organization's network, steal sensitive data, or cause system vulnerabilities.
- Data Breaches: Users might unknowingly install applications that have access to critical data, leading to potential data leaks or breaches, which could harm the organization's reputation and violate regulatory requirements.
- Compliance Issues: Organizations in regulated industries are often required to adhere to specific software standards and controls. Allowing users to install applications could lead to non-compliance with industry regulations (e.g., HIPAA, GDPR).
- System Instability: Uncontrolled installations may interfere with existing software or cause compatibility issues, leading to system crashes, poor performance, or downtime, which impacts productivity.

15. Separation of duties is best defined by policy definition. What is needed to ensure its success?

- Clear Role Definitions: The organization must clearly define roles and responsibilities for each position. Each employee should know exactly what their responsibilities are and which tasks they are authorized or prohibited from performing.
- Effective Policy Enforcement: Policies need to be enforced rigorously through procedures, audits, and regular monitoring. This includes access controls, software systems, and administrative oversight that help ensure that no one individual has the authority to perform conflicting tasks that could lead to fraud or errors.
- Monitoring and Auditing: Continuous auditing of activities within the IT systems is crucial. Automated tools or manual checks can help verify that no one individual is handling incompatible tasks or has access to sensitive data without oversight.