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: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

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}

Purpose/Objectives

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

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?}

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.}

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.}

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.}

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: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

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:

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?

3. What does separation of duties mean?

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

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

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

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

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

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

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

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

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

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

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

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