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

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 30/09/2023

PART A

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 email 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

ABC Credit Union
Policy Name: Security Management Policy with Defined Separation of Duties

Policy Statement

ABC Credit Union is committed to protecting the confidentiality, integrity, and availability of its information systems and assets. This policy establishes a framework for managing security risks and implementing a system of separation of duties to help prevent unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and assets.

Purpose/Objectives:

- Define the roles and responsibilities for information systems security throughout the seven domains of a typical IT infrastructure.
- Implement a system of separation of duties to reduce the risk of unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and assets.
- Ensure compliance with all applicable laws and regulations related to information systems security.

Scope:

- Network and communications
- Systems and applications
- Data and information
- Devices and endpoints
- Physical and environmental security
- Access control
- Security management and monitoring

Standards:

- Workstation Configuration Standards
- Server Configuration Standards
- Network Infrastructure Configuration Standards
- Database Security Standards
- Application Security Standards
- Physical Security Standards
- Access Control Standards
- Security Management and Monitoring Standards

Procedures:

- All employees, contractors, and other third parties who have access to ABC Credit Union's information systems and assets will be required to sign a non-disclosure agreement and complete security awareness training.
- Access to information systems and assets will be granted on a least privilege basis.
- A system of separation of duties will be implemented to reduce the risk of unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and assets.
- Information systems and assets will be monitored for suspicious activity and security incidents will be investigated and responded to promptly.

Guidelines:

- All changes to information systems and assets must be approved by the appropriate manager and security administrator.
- All security incidents must be reported to the security administrator immediately.
- The security administrator will investigate all security incidents and take appropriate corrective action.

PART B

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

Answer:

- User Domain
    - Educate and train users on security best practices, such as password security, phishing awareness, and social engineering.
    - Implement and maintain strong password policies.
    - Enable multi-factor authentication (MFA) for all users.
    - Monitor user activity for suspicious behavior.
    -

- Workstation Domain
    - Deploy and maintain antivirus and antimalware software on all workstations.
    - Keep workstations up to date with the latest security patches.
    - Implement and maintain strong access control policies for workstations.
    - Monitor workstation activity for suspicious behavior.

- LAN Domain
    - Implement and maintain a firewall to protect the LAN from unauthorized access.
    - Implement and maintain intrusion detection and prevention systems (IDS/IPS) to monitor the LAN for suspicious activity.
    - Segment the LAN into different networks to reduce the risk of infection spreading.
    - Monitor LAN traffic for suspicious activity.

- LAN-to-WAN Domain
    - Implement and maintain a VPN to connect the LAN to the WAN securely.
    - Implement and maintain a firewall to protect the LAN-to-WAN connection from unauthorized access.
    - Implement and maintain IDS/IPS systems to monitor the LAN-to-WAN connection for suspicious activity.
    - Monitor LAN-to-WAN traffic for suspicious activity.

- WAN Domain
    - Implement and maintain a firewall to protect the WAN from unauthorized access.
    - Implement and maintain IDS/IPS systems to monitor the WAN for suspicious activity.

- Implement and maintain traffic shaping and filtering to control WAN traffic.
- Monitor WAN traffic for suspicious activity.

- Remote Access Domain
  - Implement and maintain a VPN to allow users to connect to the network remotely.
  - Implement and maintain MFA for all remote users.
  - Implement and maintain strong access control policies for remote users.
  - Monitor remote access activity for suspicious behavior.

- System/Application Domain
  - Implement and maintain security patches for all systems and applications.
  - Implement and maintain strong access control policies for systems and applications.
  - Monitor system and application activity for suspicious behavior.

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?
Answer: The User Domain 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?
Answer: Separation of duties in IT infrastructure means that different people should be responsible for different tasks or processes. This helps to reduce the risk of fraud, error, and abuse.

4. How does separation of duties throughout an IT infrastructure mitigate risk for an organization?
Answer: Separation of duties throughout an IT infrastructure mitigates risk for an organization by reducing the opportunity for fraud, error, and abuse. When different people are responsible for different tasks or processes, it is more difficult for one person to cause damage, either intentionally or unintentionally.

5. How would you position a layered security approach with a layered security management approach for an IT infrastructure?
Answer:
- A layered security approach and a layered security management approach are two complementary approaches to securing an IT infrastructure.
- A layered security approach involves implementing multiple security controls at different layers of the IT infrastructure. This helps to protect the infrastructure from a variety of threats and attacks. For example, a layered security approach might include firewalls, intrusion detection systems, and antivirus software at the network layer; strong passwords and access control policies at the application layer; and encryption and data loss prevention at the data layer.
- A layered security management approach involves implementing multiple security management processes and procedures. This helps to ensure that the security controls in place are effective and that the IT infrastructure is being monitored and managed securely. For example, a layered security management approach might include security risk assessments, security incident response planning, and security awareness training.

- To position a layered security approach with a layered security management approach for an IT infrastructure, organizations should:

- Identify the critical assets in their IT infrastructure and the risks to those assets.
- Implement a layered security approach to protect those assets from the identified risks.
- Implement a layered security management approach to ensure that the security controls in place are effective and that the IT infrastructure is being monitored and managed securely.

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

- It would be a problem if a system administrator had both the ID and password to a system. This is because it would give them too much control over the system and could potentially allow them to cause damage, either intentionally or unintentionally
- It is important to implement separation of duties to mitigate this risk. Separation of duties means that different people should be responsible for different tasks or processes. In this case, one person should be responsible for creating and managing user accounts, and another person should be responsible for granting and revoking access to systems and applications.
- This way, no one person has too much control over any one system. By implementing separation of duties, organizations can make it more difficult for system administrators to abuse their privileges and cause damage.

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

- When using a layered security approach to system administration, the highest access privileges are typically held by a super administrator or root user. This account has the ability to make any changes to the system, including creating and deleting user accounts, installing and removing software, and modifying configuration files.
- However, it is important to note that the super administrator account should only be used for administrative tasks and should not be used for everyday activities such as checking email or browsing the web. This is because the super administrator account is a high-value target for attackers. If an attacker is able to compromise the super administrator account, they will have complete control over the system.
- To mitigate this risk, organizations should implement separation of duties for system administration tasks. This means that different people should be responsible for different tasks, such as installing and configuring software, managing user accounts, and monitoring system activity. This will help to reduce the risk of any one person being able to abuse their privileges.

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

- Chief Information Security Officer (CISO): The CISO is responsible for the overall security posture of the organization. This includes developing and implementing the organization's security strategy, as well as reviewing and approving security policies and procedures. The CISO would typically be the primary person responsible for reviewing the organization's layered approach to security.

- Security architects: Security architects are responsible for designing and implementing the organization's security architecture. This includes identifying and assessing security risks, and designing and implementing security controls to mitigate those risks. Security architects would be well-positioned to review the organization's layered approach to security and ensure that it is effective.
- Security auditors: Security auditors are responsible for conducting security assessments to identify security vulnerabilities and compliance gaps. Security auditors would be able to provide an independent review of the organization's layered approach to security and identify any areas for improvement.
- External security consultants: External security consultants can be hired to provide an independent review of the organization's layered approach to security. They can also provide advice on how to improve the organization's security posture.

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

- Technical standards are specific and measurable. This makes them easier to understand and implement. For example, a technical standard might specify the type of encryption algorithm to use or the strength of the password requirements.
- Technical standards are based on best practices. They have been developed by experts in the field of security and have been proven to be effective in protecting systems and data.
- Technical standards are vendor-neutral. This means that they are not tied to any specific product or vendor. This makes it easier for organizations to select the security solutions that best meet their needs.

10. Why is it important to define guidelines in this layered security management policy?
Answer:
It is important to define guidelines in a layered security management policy because it helps to:

- Clarify the organization's security goals and objectives. The guidelines should explain what the organization is trying to achieve with its layered security approach, and how the different layers of security work together to achieve those goals.
- Provide specific instructions on how to implement and maintain the layered security approach. The guidelines should provide clear and concise instructions on how to configure and manage the various security controls that are in place.
- Ensure consistency across the organization. The guidelines should help to ensure that the layered security approach is implemented and maintained in a consistent manner across all departments and business units.
- Improve compliance. The guidelines can help to improve compliance with security regulations and standards.

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

- To protect customer privacy. Customer privacy data is sensitive information that should only be accessed by authorized personnel. By defining access control policies, organizations can help to ensure that customer privacy data is only accessed by those who need it to do their job.

- To reduce the risk of data breaches. Data breaches can occur when unauthorized individuals gain access to sensitive data. By limiting access to customer privacy data, organizations can reduce the risk of data breaches and protect their customers' information.
- To comply with data protection regulations. Many data protection regulations, such as the General Data Protection Regulation (GDPR), require organizations to implement access control measures to protect customer privacy data.

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

- The seven domains of a typical IT infrastructure help organizations align to separation of duties because they provide a framework for dividing IT responsibilities into smaller, more manageable tasks. This makes it easier to assign different tasks to different people, which helps to reduce the risk of fraud, error, and abuse.
- By separating these tasks into different domains, organizations can make it more difficult for any one person to have too much control over any one system or process. This helps to reduce the risk of that person being able to abuse their privileges and cause damage.

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

- To ensure that the organization can continue to operate in the event of a disruption. A BCDR policy will outline the steps that the organization will take to minimize disruption to business operations in the event of a disaster or other event. This can help to reduce the financial and reputational damage that can result from a disruption.
- To comply with regulations. Many regulations require organizations to have a BCDR plan in place. For example, the Sarbanes-Oxley Act requires publicly traded companies to have a BCDR plan in place to protect their financial data.
- To protect customers and employees. A BCDR plan can help to protect customers and employees from the negative impacts of a disruption. For example, a BCDR plan may include steps to ensure that customers can still access their accounts and employees can still work even in the event of a disaster.

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

- Security risks: Applications downloaded from the internet can contain malware, such as viruses, worms, and trojans. This malware can infect the organization's network and systems, causing damage to data and systems, and disrupting business operations.
- Compliance risks: Many organizations are subject to regulations that require them to control the software that is installed on their systems. For example, the General Data Protection Regulation (GDPR) requires organizations to protect the personal data of their customers and employees. By preventing users from downloading and installing applications on their own, organizations can help to ensure that they are complying with these regulations.

- Support costs: When users download and install their own applications, it can be difficult for the IT department to support those applications. This can lead to increased support costs for the organization.
- Compatibility issues: Applications downloaded from the internet may not be compatible with the organization's systems. This can lead to problems with the applications, such as crashes and errors. This can disrupt the work of employees and reduce their productivity.

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

Answer:

Separation of duties (SoD) is an important security principle that helps to reduce the risk of fraud, error, and abuse. SoD is best defined by policy definition, but there are a number of things that are needed to ensure its success.

- Clear and concise policies: The first step to ensuring the success of SoD is to have clear and concise policies in place. These policies should define the different roles and responsibilities within the organization, and they should specify how SoD should be implemented.
- Communication and training: Once the policies are in place, it is important to communicate them to employees and provide them with training on how to comply with them. Employees need to understand their roles and responsibilities, and they need to know how to get approval for tasks that they do not have authority to perform.
- Oversight and enforcement: It is also important to have oversight and enforcement mechanisms in place to ensure that employees are complying with the SoD policies. This may involve conducting regular audits, having a process for reporting suspected violations, and disciplining employees who violate the policies.
- Technical controls: In addition to policies and procedures, technical controls can also be used to implement SoD. For example, access control lists (ACLs) can be used to restrict access to systems and data, and role-based access control (RBAC) can be used to assign specific roles and permissions to users.