Lab #3: Define an Information Systems Security Policy Framework for an IT Infrastructure

PART A: List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 23/09/2023

Overview

The following risks, threats, and vulnerabilities were found in a healthcare IT infrastructure serving patients with life-threatening situations. Given the following list, select where the risk, threat, or vulnerability resides in the seven domains of a typical IT infrastructure.

Risk – Threat – Vulnerability	Primary Domain Impacted
Unauthorized access from public Internet	LAN-to-WAN
User destroys data in application and deletes all files	System/Application
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN-to-WAN
Intra-office employee romance gone bad	User
Fire destroys primary data center	System/Application
Communication circuit outages	WAN
Workstation OS has a known software vulnerability	Workstation
Unauthorized access to organization owned Workstations	Workstation
Loss of production data	System/Application
Denial of service attack on organization e-mail Server	LAN-to-WAN
Remote communications from home office	Remote Access
LAN server OS has a known software vulnerability	LAN

User downloads an unknown e –mail attachment	User
Workstation browser has software vulnerability	Workstation
Service provider has a major network outage	WAN
Weak ingress/egress traffic filtering degrades Performance	LAN-to-WAN
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User
VPN tunneling between remote computer and ingress/egress router	LAN-to-WAN
WLAN access points are needed for LAN connectivity within a warehouse	LAN
Need to prevent rogue users from unauthorized WLAN access	LAN

Part B: List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

Risk – Threat – Vulnerability	Policy Definition Required
Unauthorized access from public Internet	Internet Ingress/Egress Traffic Policy Definition
User destroys data in application and deletes all files	Data Classification Standard & Encryption Policy Definition
Hacker penetrates your IT infrastructure and gains access to your internal network	Access Control Policy Definition
Intra-office employee romance gone bad	Access Control Policy Definition
Fire destroys primary data center	Business Continuity & Disaster Recovery Policy Definition
Communication circuit outages	WAN Service Availability Policy Definition
Workstation OS has a known software vulnerability	Vulnerability Management & Vulnerability Window Policy Definition
Unauthorized access to organization owned Workstations	Access Control Policy Definition
Loss of production data	Production Data Back-up Policy

	Definition
Denial of service attack on organization e-mail Server	Access Control Policy Definition
Remote communications from home office	Access Control Policy Definition
LAN server OS has a known software vulnerability	Vulnerability Management & Vulnerability Window Policy Definition
User downloads an unknown e –mail attachment	Mandated Security Awareness Training Policy Definition
Workstation browser has software vulnerability	Vulnerability Management & Vulnerability Window Policy Definition
Service provider has a major network outage	Business Continuity & Disaster Recovery Policy Definition
Weak ingress/egress traffic filtering degrades Performance	Internet Ingress/Egress Traffic Policy Definition
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	Acceptable Use Policy
VPN tunneling between remote computer and ingress/egress router	Remote Access Policy Definition
WLAN access points are needed for LAN connectivity within a warehouse	Access Control Policy Definition
Need to prevent rogue users from unauthorized WLAN access	Access Control Policy Definition

Part C: Define an Information Systems Security Policy Framework for an IT Infrastructure

Lab Assessment Questions & Answers

1. A policy definition usually contains what four major parts or elements?
Answer:

1. A policy definition usually contains the following four major parts or elements: Problem identification: This section identifies the problem or issue that the policy is designed to address. It is important to clearly and concisely define the problem so that the policy can be tailored to address it effectively.
2. Policy formulation: This section outlines the specific actions or steps that will be taken to address the problem identified in the first section. The policy should be clear, concise, and easy to understand, and it should be written in a way that is enforceable.

3. Adoption: This section describes the process by which the policy will be adopted or approved. This may involve a vote by a governing body, the signature of a senior executive, or some other form of approval.
4. Implementation: This section describes how the policy will be put into practice. This may involve developing procedures, training staff, and creating communication materials.

2. In order to effectively implement a policy framework, what three organizational elements are absolutely needed to ensure successful implementation?
Answer:
To effectively implement a policy framework, the following three organizational elements are absolutely needed to ensure successful implementation:

- Leadership commitment: Top management must be committed to the policy and to its successful implementation. This commitment must be demonstrated through words and actions, such as providing adequate resources, supporting staff training, and holding employees accountable for compliance.
- Clear communication: The policy must be clearly communicated to all affected employees. This communication should take place at all levels of the organization and should be ongoing. Employees should understand the purpose of the policy, their individual responsibilities, and the consequences of non-compliance.
- Effective monitoring and evaluation: The policy must be monitored and evaluated on a regular basis to ensure that it is being implemented effectively and achieving its desired results. This monitoring and evaluation should be conducted by a neutral party, such as an internal audit team or an external consultant.

3. Which policy is the most important one to implement to separate employer from employee? Which is the most challenging to implement successfully?
Answer:
The most important policy to implement to separate employer from employee is a confidentiality policy. This policy should clearly define what information is considered confidential and how it should be protected. It should also outline the consequences of violating the confidentiality policy.
A confidentiality policy is important because it helps to protect the employer's trade secrets, proprietary information, and customer data. It also helps to protect the employee's privacy.
The most challenging policy to implement successfully is a conflict of interest policy. This policy should identify potential conflicts of interest and how they should be managed. It should also outline the consequences of failing to manage a conflict of interest.
A conflict of interest policy is challenging to implement because it can be difficult to identify all potential conflicts of interest. Additionally, employees may be reluctant to report conflicts of interest for fear of being disciplined or terminated.

4. Which domain requires stringent access controls and encryption for connectivity to the corporate resources from home? What policy definition is needed for this domain?
Answer:
The domain that requires stringent access controls and encryption for connectivity to corporate resources from home is the remote access domain. This domain includes all of the systems and applications that employees need to access in order to work from home.

A policy definition for this domain should include the following:

- Who is authorized to access remote resources? This should be clearly defined and limited to employees who have a legitimate need to access these resources.
- What devices and software are authorized to access remote resources? This should also be clearly defined and limited to devices and software that are known to be secure.
- What methods of authentication are required to access remote resources? This should include strong multi-factor authentication (MFA).
- What encryption methods are required to protect data in transit and at rest? This should include strong encryption methods, such as AES-256.
- How are remote access devices and software managed and secured? This should include regular patching and updates, as well as security monitoring.

5. Which domains need software vulnerability management & vulnerability window policy definitions to mitigate risk from software vulnerabilities?
Answer:
All 7 domains in the 7 domains of IT infrastructure need software vulnerability management and vulnerability window policy definitions to mitigate risk from software vulnerabilities.
Software vulnerabilities can be exploited by attackers to gain unauthorized access to systems and data, disrupt operations, or steal intellectual property. By implementing software vulnerability management and vulnerability window policy definitions, organizations can help to reduce their risk from software vulnerabilities in all of these domains.

6. Which domain requires AUPs to minimize unnecessary User-initiated Internet traffic and awareness of the proper use of organization-owned IT assets?
Answer:
The domain that requires AUPs to minimize unnecessary User-initiated Internet traffic and awareness of the proper use of organization-owned IT assets is the User Domain.
The User Domain includes all of the end users of the organization's IT infrastructure, including employees, contractors, and guests. These users are responsible for using the organization's IT assets in a responsible and ethical manner.
An Acceptable Use Policy (AUP) is a document that outlines the acceptable and unacceptable uses of an organization's IT assets. The AUP should be clear and concise, and it should be communicated to all users.

7. What policy definition can help remind employees within the User Domain about on-going acceptable use and unacceptable use?
Answer:
The policy definition that can help remind employees within the User Domain about on-going acceptable use and unacceptable use is the Acceptable Use Policy (AUP).
The AUP should be a living document that is regularly reviewed and updated to reflect changes in technology and the organization's needs. The AUP should also be communicated to employees in a variety of ways, such as through email, training sessions, and posters.

8. What policy definition is required to restrict and prevent unauthorized access to organization owned IT systems and applications?
Answer:

This policy should define who is authorized to access the organization's IT systems and applications, and what level of access they should have. The policy should also define the methods that will be used to control access, such as passwords, multi-factor authentication, and role-based access control (RBAC).
The Access Control Policy should be implemented using a combination of technical and administrative controls. Technical controls, such as firewalls and intrusion detection systems, can be used to restrict access to the organization's IT infrastructure. Administrative controls, such as employee training and background checks, can be used to reduce the risk of unauthorized access from within the organization.

9. What is the relationship between an Encryption Policy Definition and a Data Classification Standard?
Answer:
The relationship between an encryption policy definition and a data classification standard is that the encryption policy definition should be based on the data classification standard. In other words, the encryption policy definition should specify that all data at a certain sensitivity level or higher must be encrypted.

10. What policy definition is needed to minimize data loss?
Answer:
A DLP policy should include the following elements:

- Data classification: The policy should define the different types of data that are subject to the policy and classify them according to their sensitivity.
- Data protection: The policy should specify the measures that will be taken to protect data at rest and in transit. This may include encryption, access controls, and auditing.
- Data monitoring: The policy should specify how data will be monitored for unauthorized access, use, or disclosure. This may involve using security software or manual reviews.
- Incident response: The policy should define how the organization will respond to data loss incidents. This may involve notifying affected individuals, investigating the incident, and taking corrective action.

11. Explain the relationship between the policy-standard-procedure-guideline structure and how this should be postured to the employees and authorized users
Answer:
Standards are more specific and detailed than policies. They define the specific requirements that must be met in order to achieve the organization's goals.
Procedures are step-by-step instructions on how to perform specific tasks. They are typically used to implement standards and policies.
Guidelines are recommendations or best practices for performing tasks. They are not mandatory, but they can be used to help employees and authorized users understand how to comply with policies and standards.
The PSPG structure should be postured to employees and authorized users in a way that is clear, concise, and easy to understand. The organization should provide training on the PSPG structure and how to use it to find the information they need.

12. Why should an organization have a remote access policy even if they already have an Acceptable Use Policy (AUP) for employees?

Answer:

Some of the reasons why organizations should have a separate remote access policy:

- Remote access can introduce new security risks. When employees access corporate resources from outside the office, they may be doing so from less secure networks, such as public Wi-Fi networks. This can make it easier for attackers to intercept data or gain access to corporate systems.
- A remote access policy can help to mitigate these risks. By implementing a remote access policy, organizations can require employees to use strong passwords, enable multi-factor authentication, and connect to corporate resources using a secure VPN connection.
- A remote access policy can help to ensure compliance with regulations. Many industries have regulations that govern how sensitive data can be accessed and transmitted. A remote access policy can help organizations to comply with these regulations.
- A remote access policy can help to improve the employee experience. A remote access policy can provide clear guidance to employees on how to access corporate resources from home. This can help to save employees time and frustration.

13. What security controls can be implemented on your e-mail system to help prevent rogue or malicious software disguised as URL links or e-mail attachments from attacking the Workstation Domain? What kind of policy definition should this be included in? Justify your answer.

Answer:

The following security controls can be implemented on an email system to help prevent rogue or malicious software disguised as URL links or email attachments from attacking the Workstation Domain:

- Email filtering: Email filters can be used to scan incoming and outgoing emails for malicious content, such as viruses, malware, and phishing attacks.
- Spam filtering: Spam filters can be used to block spam emails, which are often used to distribute malware.
- Sandboxing: Sandboxing is a technique that allows emails to be executed in a safe and isolated environment. This can help to prevent malicious emails from executing and harming the Workstation Domain.
- Multi-factor authentication (MFA): MFA can be used to add an extra layer of security to email logins. This can help to prevent unauthorized access to email accounts, which could be used to send malicious emails.
- These security controls should be included in an email security policy. This policy should define the organization's requirements for email security, including the use of email filters, spam filters, sandboxing, and MFA. The policy should also define the consequences of violating the policy.

Justification:

Email is a common vector for malware attacks. Attackers often use email to send malicious attachments or links to phishing websites. By implementing the security controls listed above, organizations can help to protect themselves from these attacks.

An email security policy is important because it helps to ensure that all employees are aware of the organization's requirements for email security. The policy also helps to define the

consequences of violating the policy, which can help to deter employees from engaging in risky behavior.

14. Why should an organization have annual security awareness training that includes an overview of the organization's policies?
Answer:
Organizations should have annual security awareness training that includes an overview of the organization's policies for the following reasons:

- To keep employees up-to-date on the latest security threats and best practices. Security threats are constantly evolving, so it is important to keep employees up-to-date on the latest threats and how to protect themselves from them.
- To reinforce the organization's security policies. Security awareness training can help to remind employees of the organization's security policies and why they are important.
- To help employees understand their role in protecting the organization. Security awareness training can help employees to understand how their actions can impact the security of the organization and how they can help to protect the organization's assets.
- To reduce the risk of security incidents. Security awareness training can help to reduce the risk of security incidents by teaching employees how to identify and avoid common security threats.

15. What is the purpose of defining of a framework for IT security policies?
Answer:
The purpose of defining a framework for IT security policies is to provide a comprehensive and structured approach to managing IT security risks. A framework provides a set of principles, best practices, and standards that organizations can use to develop and implement effective security policies.

A well-defined IT security framework can help organizations to:

- Identify and assess their IT security risks. By understanding their risks, organizations can prioritize their security efforts and implement the most appropriate controls.
- Develop and implement effective security policies. A framework can provide guidance on what policies are needed and how to implement them.
- Ensure compliance with regulations. Many industries have regulations that require organizations to implement certain security controls. A framework can help organizations to ensure that they are in compliance with these regulations.
- Improve their security posture. A framework can help organizations to identify and implement the security controls that are needed to protect their IT assets.