Laboratory #3

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

Learning Objectives and Outcomes

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

- Identify risks and threats commonly found within the seven domains of a typical IT infrastructure
- Define security policies to address each identified risk and threat as they are organized within the seven domains of a typical IT infrastructure
- Align security policies to mitigate risks from threats and vulnerabilities found within the seven domains of a typical IT infrastructure
- Organize the security policies within an overall framework as part of an overall layered security strategy for the seven domains of a typical IT infrastructure
- Select the appropriate policy definitions needed throughout the seven domains of a typical IT infrastructure to mitigate the identified risks, threats, and vulnerabilities

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 #3:

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 #3 – Student Steps

The student steps that are needed to perform Lab #3: Define the Scope & Structure for an IT Risk Management Plan are listed here:

1. Review the seven domains of a typical IT infrastructure and identify common risks, threats, and vulnerabilities

2. Complete the Lab #3 – Assessment Worksheet, Part A on common risks, threats, and vulnerabilities found
3. Review how can these risks, threats, and vulnerabilities may be mitigated through policy definition within the seven domains of a typical IT infrastructure
4. Complete the Lab #3 – Assessment Worksheet, Part B on selecting policy definitions that may help mitigate the risks, threats, and vulnerabilities identified throughout the seven domains of a typical IT infrastructure
5. Answer Lab #3 – Assessment Questions & Answers and submit as part of your Lab #3 deliverables

Deliverables

Upon completion of Lab 3: Define an Information Systems Security Policy Framework for an IT Infrastructure, the students are required to provide the following deliverables as part of this lab:

1. Lab #3 – Assessment Worksheet, Part A
2. Lab #3 – Assessment Worksheet, Part B
3. Lab #3 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #3 that the students must perform:

1. Was the student able to identify risks and threats commonly found within the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to define security policies to address each identified risk and threat within the seven domains of a typical IT infrastructure? – [**20%**]
3. Was the student able to align security policies to mitigate risks from threats and vulnerabilities found within the seven domains of a typical IT infrastructure? – [**20%**]
4. Was the student able to organize security policies within an overall framework as part of an overall layered security strategy for the seven domains of a typical IT infrastructure? – [**20%]**
5. Was the student able to select appropriate policy definitions needed throughout the seven domains of a typical IT infrastructure to mitigate the identified risks, threats, and vulnerabilities? – [**20%**]

Lab #3 – Assessment Worksheet

Part A – List of Risks, Threats, and Vulnerabilities Commonly Found in an IT Infrastructure

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

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	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance "gone bad"	
Fire destroys the primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail server	

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

Lab #3 – Assessment Worksheet

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

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

For each of the identified risks, threats, and vulnerabilities; select the most appropriate policy definition that may help mitigate the identified risk, threat, or vulnerability within that domain from the following list:

Policy Definition List

Acceptable Use Policy

Access Control Policy Definition

Business Continuity – Business Impact Analysis (BIA) Policy Definition

Business Continuity & Disaster Recovery Policy Definition

Data Classification Standard & Encryption Policy Definition

Internet Ingress/Egress Traffic Policy Definition

Mandated Security Awareness Training Policy Definition

Production Data Back-up Policy Definition

Remote Access Policy Definition

Vulnerability Management & Vulnerability Window Policy Definition

WAN Service Availability Policy Definition

Risk – Threat – Vulnerability	Policy Definition Required
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization-owned Workstations	
Loss of production data	
Denial of service attack on organization e-mail Server	
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades Performance	

Risk – Threat – Vulnerability	Policy Definition Required
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

Lab #3 – Assessment Worksheet

Define an Information Systems Security Policy Framework for an IT Infrastructure

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, students identified risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure. By organizing these risks, threats, and vulnerabilities within each of the seven domains of a typical IT infrastructure information system security policies can be defined to help mitigate this risk. Using policy definition and policy implementation, organizations can "tighten" security throughout the seven domains of a typical IT infrastructure.

Lab Assessment Questions & Answers

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

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

3. Which policy is the most important one to implement to separate employer from employee? Which is the most challenging to implement successfully?

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?

5. Which domains need software vulnerability management & vulnerability window policy definitions to mitigate risk from software vulnerabilities?

6. Which domain requires AUPs to minimize unnecessary User-initiated Internet traffic and awareness of the proper use of organization-owned IT assets?

7. What policy definition can help remind employees within the User Domain about on-going acceptable use and unacceptable use?

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

9. What is the relationship between an Encryption Policy Definition and a Data Classification Standard?

10. What policy definition is needed to minimize data loss?

11. Explain the relationship between the policy-standard-procedure-guideline structure and how this should be postured to the employees and authorized users.

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

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.

14. Why should an organization have annual security awareness training that includes an overview of the organization's policies?

15. What is the purpose of defining of a framework for IT security policies?