Course Name: IAP301
Student Name: Dang Hoang Nguyen
Instructor Name: Mai Hoang Dinh
Lab Due Date: 18/1/2024

Risk – Threat – Vulnerability	**Primary Domain Impacted**
Unauthorized access from public Internet	Remote access Domain
User destroys data in application and **deletes all files**	System/Application Domain
Hacker penetrates your IT infrastructure and gains access to your **internal network**	LAN to WAN Domain
Intra-office employee romance gone bad	User Domain
Fire destroys primary **data center**	System/Application Domain
Communication circuit outages	WAN Domain
Workstation OS has a known **software vulnerability**	Workstation Domain
Unauthorized access to organization owned **Workstations**	Workstation Domain
Loss of production **data**	System/Application Domain
Denial of service attack on organization e-mail Server	LAN to WAN Domain
Remote communications from home office	Remote Access Domain
LAN server OS has a **known software vulnerability**	LAN Domain
User downloads an unknown e –mail attachment	User Domain
Workstation browser has software vulnerability	Workstation Domain
Service provider has **a major network** outage	WAN Domain
Weak ingress/egress traffic filtering degrades **Performance**	LAN to WAN Domain
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User Domain
VPN tunneling between **remote computer** and **ingress/egress router**	LAN to WAN Domain
WLAN access points are needed for LAN connectivity **within a warehouse**	LAN Domain
Need to **prevent rogue users** from unauthorized WLAN access	LAN Domain

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 and Encryption Policy Definition
Hacker penetrates your IT infrastructure and gains access to your **internal network**	Vulnerability Management and Vulnerability Window Policy Definition
Intra-office employee romance gone bad	Mandated Security Awareness Training Policy Definition
Fire destroys primary **data center**	Business Continuity and Disaster Recovery Policy Definition
Communication circuit outages	Business Continuity - Business Impact analysis (BIA) Policy Definition
Workstation OS has a known **software vulnerability**	Production Data Backup Policy Definition
Unauthorized access to organization owned **Workstations**	Access Control Policy
Loss of production **data**	Production Data Backup Policy Definition
Denial of service attack on organization e-mail Server	Internet Ingress/Egress Traffic Policy Definition
Remote communications from home office	Remote Access Policy Definition
LAN server OS has a **known software vulnerability**	Vulnerability Management and Vulnerability Window Policy Definition
User downloads an unknown e –mail attachment	Acceptable Use Policy
Workstation browser has software vulnerability	Vulnerability Management and Vulnerability Window Policy Definition
Service provider has **a major network** outage	WAN Service Availability 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**	WAN service Availability Policy Definition
Need to **prevent rogue users** from unauthorized WLAN access	Access Control Policy Definition

Lab Assessment Question & Answers

1. A policy definition usually contains what for major part or elements?
Problem identification, Policy formulation, Adoption, Implementation.

2. In order to effectively implement a policy framework, what three organizational elements are absolutely needed to ensure successful implementation?
Critical to his approach is the definition of policies, standards and technical controls aligned.

3. Which policy is the most important one to implement to separate employer from employee? which is the most challenging to implement successfully
The master policy is the important one to implement that are separate from employer from employee. The most challenging is acceptable use policy.

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?
The remote desktop requires stringent access controls and encryption for connection to the corporate resources from home. This domain needs the access control policy definition.

5. Which domains need software vulnerability management & vulnerability window policy definitions to mitigate risk from software vulnerabilities?
The user domain, workstation domain, and the LAN domain

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

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

The AUP can help remind employees about on-going acceptable use and unacceptable use.
8. What policy definition is required so restrict and prevent unauthorized access to organization owned IT systems and applications?
the access control policy definition

9. What is the relationship between an Encryption Policy Definition and a Data Classification Standard?
They both help classify sensitive data and help secure it from unauthorized access

10. What policy definition is needed to minimize data loss?
The data classification standard and encryption policy

11. Explain the relationship between the policy-standard-procedure- guideline structure and how this should be postured to the employees and authorized users.
The policy-standard-procedure-guideline structure gives the organization a more organized method of creating a policy.

12. Why should an organization have a remote access policy event of they already have an Acceptable Use Policy (AUP) for employees?
Because remote access is on an open connection and it make more dangerous to the organization

13. What security controls can be implemented on 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.
Should disable click links and attachments from outside. This should be included in the AUP or the Internet Egress/Ingress policy definition.

14.Why should an organization have annual security awareness training that includes an overview of the organization's policies?
They should do this to remind employees of the policies and to inform them in any updates to the policies.

15. What is the purpose of definition of a framework for IT security policies?
The purpose is to give the creator of the policies some guidelines and an idea of what they should follow to keep their organization safe and secure.

Lab #1: Assessment Worksheet

Identify Threats and Vulnerabilities in an IT Infrastructure

Course Name: IAA202
Student Name: Dang Hoang Nguyen
Instructor Name: Mrs. Pham Yen Thao
Lab Due Date: May 13, 2023

Overview

One of the most important first steps to risk management and implementing a risk mitigation strategy is to identify known risks, threats, and vulnerabilities and organize them. The purpose of the seven domains of a typical IT infrastructure is to help organize the roles, responsibilities, and accountabilities for risk management and risk mitigation. This lab requires students to identify risks, threats, and vulnerabilities and map them to the domain that these impact from a risk management perspective.

Lab Assessment Questions

Given the scenario of a healthcare organization, answer the following Lab #1 assessment questions from a risk management perspective:

1. Healthcare organizations are under strict compliance to HIPPA privacy requirements which require that an organization have proper security controls for handling personal healthcare information (PHI) privacy data. This includes security controls for the IT infrastructure handling PHI privacy data. Which one of the listed risks, threats, or vulnerabilities can violate HIPPA privacy requirements? List one and justify your answer in one or two sentences.

   I think that is "Unauthorized access to organization owned Workstations". Because when a workstation that contain all the PHI of the patient and accessed by an Unauthorized user. This could lead to the leak of security data breach and put the privacy of the patient at risk (HIPPA violation)

2. How many threats and vulnerabilities did you find that impacted risk within each of the seven domains of a typical IT infrastructure?

   User Domain: 03

   Workstation Domain: 03

   LAN Domain: 03

   LAN-to-WAN Domain: 04

   WAN Domain: 02

   Remote Access Domain: 02

   Systems/Application Domain: 03

3. Which domain(s) had the greatest number of risks, threats, and vulnerabilities?

   LAN to WAN Domain

4. What is the risk impact or risk factor (critical, major, minor) that you would qualitatively assign to the risks, threats, and vulnerabilities you identified for the LAN-to-WAN Domain for the healthcare and HIPPA compliance scenario?

Risk – Threat – Vulnerability	**Risk impact or risk factor**
Hacker penetrates your IT infrastructure and gains access to your internal network.	Critical. Because hacker can get access to data security breach
Denial of service attack on organization e-mail Server	Three of them, depend on the situation. Hacker can make disruption of business operation, data breach or financial loss
Weak ingress/egress traffic filtering degrades Performance.	Minor to major. Minor: reduce the performance

	Major: security risk, compliance violation
VPN tunneling between remote computer and ingress/egress router.	Major: Error when configurating → get network's vulnerable to attack by malware, etc. Insider threat, communication interception

5. Of the three Systems/Application Domain risks, threats, and vulnerabilities identified, which one requires a disaster recovery plan and business continuity plan to maintain continued operations during a catastrophic outage?

   Fire destroys data center

6. Which domain represents the greatest risk and uncertainty to an organization?

   User Domain

7. Which domain requires stringent access controls and encryption for connectivity to corporate resources from home?

   Remote Access Domain

8. Which domain requires annual security awareness training and employee background checks for sensitive positions to help mitigate risk from employee sabotage?

   User Domain

9. Which domains need software vulnerability assessments to mitigate risk from software vulnerabilities?

   System/Application and LAN to WAN domains

10. Which domain requires AUPs to minimize unnecessary User initiated Internet traffic and can be monitored and controlled by web content filters?

    User Domain

11. In which domain do you implement web content filters?

    LAN to WAN Domain

12. If you implement a wireless LAN (WLAN) to support connectivity for laptops in the Workstation Domain, which domain does WLAN fall within?

    LAN Domain

13. A bank under Gramm-Leach-Bliley-Act (GLBA) for protecting customer privacy has just implemented their online banking solution allowing customers to access their accounts and perform transactions via their computer or PDA device. Online banking servers and their public Internet hosting would fall within which domains of security responsibility?

    It would fall within WAN as well as Remote Access Domains of security responsibility.

14. Customers that conduct online banking using their laptop or personal computer must use HTTPS:, the secure and encrypted version of HTTP: browser communications. HTTPS:// encrypts webpage data inputs and data through the public Internet and decrypts that webpage and data once displayed on your browser. True or False.

    True. HTTPS encrypts webpage data inputs and data through the public Internet and decrypts that webpage and data once displayed on your browser.

15. Explain how a layered security strategy throughout the 7-domains of a typical IT infrastructure can help mitigate risk exposure for loss of privacy data or confidential data from the Systems/Application Domain.

    By integrating several security controls at various layers of the infrastructure, a layered security approach throughout the seven domains of a typical IT infrastructure

can assist reduce the risk exposure for loss of privacy data or secret data from the Systems/Application Domain. To offer defense-in-depth and lessen the risk and consequence of a security breach, various domains can install access controls, encryption, firewalls, intrusion detection/prevention systems, monitoring, and logging.