Lab #10: Align an IT Security Policy Framework to the 7 Domains of a Typical IT

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 28/10/2023

Part A – Policy Statement Definitions

Overview

Create a policy statement that defines how these policies mitigate the risk, threat, or vulnerability as indicated in the gap analysis matrix below for each of the gaps identified and recommended policy definitions

Risk – Threat – Vulnerability	IT Security Policy Definition
Unauthorized access from public Internet	Implement a firewall and intrusion detection system to monitor and block unauthorized access from the public Internet.
User destroys data in application and deletes all files	Implement data access controls to prevent unauthorized users from accessing or destroying data.
Hacker penetrates your IT infrastructure and gains access to your internal network	Implement network segmentation to isolate critical systems and data from the rest of the network.
Intra-office employee romance gone bad	Implement access control procedures to prevent unauthorized access to systems and data.
Fire destroys primary data center	Implement a data backup and redundancy plan to ensure that data is not lost in the event of a disaster.
Communication circuit outages	Implement redundant communication circuits to ensure that business operations can continue in the event of an outage.
Workstation OS has a known software vulnerability	Implement a patch management process to ensure that all systems are up-to-date with the latest security patches.
Unauthorized access to organization owned Workstations	Implement physical access control measures to prevent unauthorized access to organization-owned workstations.
Loss of production data	Implement a data backup and redundancy plan to ensure that data is not lost in the event of a failure.
Denial of service attack on organization e-mail Server	Implement email server protection measures to mitigate denial of service attacks.
Remote communications from home office	Implement a VPN solution to provide secure remote access to the organization's network.
LAN server OS has a known software vulnerability	Implement a patch management process to ensure that all systems are up-to-date with the latest security patches.
User downloads an unknown e-mail attachment	Implement email security measures to block malicious attachments.
Workstation browser has software vulnerability	Implement a patch management process to ensure that all systems are up-to-date with the latest security

	patches.
Service provider has a major network outage	Implement redundant service provider connections to ensure that business operations can continue in the event of an outage.
Weak ingress/egress traffic filtering degrades Performance	Implement ingress/egress traffic filtering to block malicious traffic and improve performance.
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	Implement a removable media policy to restrict the use of removable media.
VPN tunneling between remote computer and ingress/egress router	Implement a VPN policy to define the requirements for VPN usage.
WLAN access points are needed for LAN connectivity within a warehouse	Implement wireless security measures to secure the WLAN network.
Need to prevent rogue users from unauthorized WLAN access	Implement rogue AP detection to detect and block unauthorized WLAN access points.

For each identified gap, insert a recommendation for an IT security policy to help mitigate the risk, threat or vulnerability:
Define a policy statement (2 or 3 sentences max) for each of the following policy definitions that are needed to remediate the identified gap analysis for the IT security policy framework:

1. Access Control Policy Definition: The organization shall implement an access control policy to ensure that only authorized personnel have access to its information assets. Access control policies shall be based on the principle of least privilege.

2. Business Continuity - Business Impact Analysis (BIA) Policy Definition: The organization shall implement a business continuity plan that includes a business impact analysis (BIA) to identify critical business processes and their dependencies. The BIA shall be reviewed regularly to ensure its effectiveness.

3. Business Continuity & Disaster Recovery Policy Definition: The organization shall implement a comprehensive business continuity and disaster recovery plan to ensure that critical business processes can be restored in the event of a disaster. The plan shall include offsite backup of critical data and redundant systems at an alternate location.

4. Data **Classification Standard & Encryption Policy Definition:** The organization shall implement a data classification standard to ensure that all information assets are classified according to their sensitivity level. Encryption policies shall be based on the sensitivity level of the data.

5. Internet Ingress/Egress Traffic & Web Content Filter Policy Definition: The organization shall implement an internet ingress/egress traffic and web content filter policy to restrict access to malicious websites and prevent unauthorized access from the public internet.

6. Production Data Back-up Policy Definition: The organization shall implement a data backup and recovery system to ensure that critical production data is not lost due to accidental or intentional deletion. The backup system shall be tested regularly to ensure its effectiveness.

7. Remote Access VPN Policy Definition: The organization shall implement a remote access virtual private network (VPN) policy to allow remote employees to securely connect to the internal network. All remote communications shall be encrypted using strong encryption algorithms.

8. WAN Service Availability Policy Definition: The organization shall implement a wide area network (WAN) service availability policy to ensure that critical communication channels are always available. This shall include but not be limited to voice, data, and video communication channels.

9. Internet Ingress/Egress Availability (DoS/DDoS) Policy Definition: The organization shall implement an internet ingress/egress availability policy to prevent denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on its network infrastructure.

10. Wireless LAN Access Control & Authentication Policy Definition: The organization shall implement a wireless LAN access control and authentication policy to restrict access only to authorized users. Access control policies for WLANs shall be based on the principle of least privilege.

11. Internet & E-Mail Acceptable Use Policy Definition: The organization shall implement an internet and e-mail acceptable use policy that defines acceptable use of company-owned IT resources by employees, contractors, and third-party vendors.

12. Asset Protection Policy Definition: The organization shall implement an asset protection policy that defines procedures for protecting company-owned IT assets from theft, damage, or loss.

13. Audit & Monitoring Policy Definition: The organization shall implement an audit and monitoring policy that defines procedures for monitoring IT systems for security breaches, unauthorized access, or other security incidents.

14. Computer Security Incident Response Team (CSIRT) Policy Definition: The organization shall implement a computer security incident response team (CSIRT) policy that defines procedures for responding to security incidents, including but not limited to virus outbreaks, hacking attempts, and denial-of-service attacks.

15. Security Awareness Training Policy Definition: The organization shall implement a security awareness training policy that requires all employees, contractors, and third-party vendors to receive regular training on information security best practices.

Part B – Craft an IT Security Policy Definition

Overview

In this lab, you are to create an organization-wide policy defining from the list provided in Lab #10 – Part A. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and 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 for 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 use of the e-mail system by implementing e-mail security controls
- The organization wants to fill the gaps identified in the IT security policy framework definition
- Select one of the identified policy definitions from the gap analysis and define an entire IT security policy definition for this needed policy definition

Instructions

Using Microsoft Word, create an IT security policy definition of your choice to mitigate the risks, threats, and vulnerabilities identified in the gap analysis. Use the following policy template:

ABC Credit Union
Remote Access VPN Policy

Policy Statement

The purpose of this policy is to define the organization's requirements for remote access to its network. The policy is designed to protect the organization from unauthorized access and to ensure that only authorized users can access its network.

Purpose/Objectives

- Unauthorized access to the organization's network and data
- Denial of service attacks
- Introduction of malware onto the organization's network
- Data loss

This policy will help to mitigate these risks by:

- Requiring all remote access users to use a VPN connection
- Implementing strong authentication and authorization controls for remote access users
- Monitoring remote access traffic for suspicious activity

Scope

The following Seven Domains of a typical IT infrastructure are impacted by this policy:

- Access Control: The policy defines the requirements for authentication and authorization for remote access users.
- Asset Management: The policy defines the requirements for managing and protecting remote access devices.
- Audit and Accountability: The policy defines the requirements for auditing and monitoring remote access activity.
- Awareness and Training: The policy defines the requirements for training remote access users on security best practices.
- Business Continuity and Disaster Recovery: The policy defines the requirements for maintaining business continuity in the event of a disruption to remote access.
- Data Protection: The policy defines the requirements for protecting data accessed remotely.
- Incident Response: The policy defines the requirements for responding to security incidents involving remote access.

The following elements or IT assets or organization-owned assets are within the scope of this policy:

- All remote access devices, including laptops, tablets, and smartphones
- All data accessed remotely, including customer data, financial data, and intellectual property

Standards

- NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations
- ISO/IEC 27001:2013: Information Security Management Systems - Requirements

Procedures

- All remote access users will be required to use a VPN connection to access the organization's network.
- All remote access users will be required to use strong authentication credentials, such as a multi-factor authentication solution.
- All remote access traffic will be monitored for suspicious activity.
- Remote access users will be required to complete security awareness training on an annual basis.

Guidelines

- The organization will provide remote access users with a list of approved VPN clients.
- The organization will provide remote access users with instructions on how to configure their devices to use the VPN.
- The organization will monitor remote access traffic using a security information and event management (SIEM) system.
- The organization will provide remote access users with security awareness training on topics such as phishing, malware, and social engineering.