Laboratory #6

Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics

Learning Objectives and Outcomes

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

- Define the scope of an remote access policy as it relates to the Remote Access Domain
- Identify the key elements of a remote access policy within an organization as part of an overall security management framework
- Align the remote access policy with the organization's goals for compliance
- Mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition
- Create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines

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 #6:

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 #6 – Student Steps

1. Review with the instructor sample Remote Access Policy documents found on the Internet:
   SANS Institute: Remote Access Policy Template
   http://www.sans.org/security-resources/policies/Remote_Access_Policy.pdf

   Higher-Education: Clark University
   http://www.clarku.edu/offices/its/policies/remoteaccess.cfm

Higher-Education: Purdue University
http://www.purdue.edu/policies/pages/information_technology/v_1_6.shtml

Healthcare: UNC School of Medicine & Healthcare Clinic
http://www.med.unc.edu/security/hipaa/documents/SOM%20Remote%20Access%20Policy%202009%20Final.pdf

2. Discuss what the risks and threats are within the Remote Access Domain per the bulleted list provided:
   - Brute force user ID and password attacks
   - Users or employees unaware of the risks, threats, and dangers of the Internet and shared Wi-Fi or broadband Internet access
   - Multiple access attempts and login retries
   - Unauthorized access to IT systems, applications, and data
   - Privacy data or confidential data is compromised remotely
   - Data leakage occurs in violation of Data Classification Standard
   - Remote worker's laptop is stolen
   - Remote worker's token device is stolen
   - Remote worker requires access to patient medical records system through public Internet
3. Discuss what organizations can do to mitigate the risks and threats identified within the Remote Access Domain
4. Complete the Lab #6 – Assessment Worksheet deliverables: Identify Elements of a Remote Access Policy Definition, Create a Remote Access Policy Definition for Multiple Healthcare Clinics
5. Complete the Lab #6 – Assessment Questions & Answers and submit with this lab.

Deliverables

Upon completion of the Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics, the students are required to provide the following deliverables:

1. Lab #6 – Assessment Worksheet: Identify Elements of a Remote Access Policy Definition
2. Lab #6 – Assessment Worksheet: Create a Remote Access Policy Definition for Multiple Remote Healthcare Clinics
3. Lab #6 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #6 that the students must demonstrate:

1. Was the student able to define the scope of a remote access policy as it relates to the Remote Access Domain? – [**20%**]
2. Was the student able to identify the key elements of remote access policy within an organization as part of an overall security management framework? – [**20%**]
3. Was the student able to align the remote access policy with the organization's goals for compliance? – [**20%**]
4. Was the student able to mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition? - [**20%**]
5. Was the student able to create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines? – [**20%**]

Lab #6 – Assessment Worksheet

Elements of a Remote Access Domain Policy

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: ______________________

Lab Due Date: ______________________

Overview

For each of the identified risks and threats within the Remote Access Domain, identify a security control or security countermeasure that can help mitigate the risk or threat. These security controls or security countermeasures will become the basis of the scope of the Remote Access Domain Policy definition to help mitigate the risks and threats commonly found within the Remote Access Domain.

Remote Access Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Brute force user ID and password attacks	Limit the request login about 5 times. Using complex passwor
Multiple login retries and access control attacks	Limit the request login
Unauthorized remote access to IT systems, applications, and data	Using ID and password for login request
Privacy data or confidential data is compromised remotely	Encrypt or using VPN for more secure data
Data leakage in violation of existing Data Classification Standards	Encrypt the input data withkey that only the administrator can decrypt

Remote Access Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Mobile worker laptop is stolen	Using camera for more secure, using locker to lock the devices when users not use
Mobile worker token or other lost or stolen authentication device	Lock that user to limited the access, until find the token or authentication device.Administrator can create the new authentication if it necessary
Remote worker requires remote access to medical patient online system through the public Internet	Using VPN for more secure connection
Users and employees are unaware of the risks and threats caused by the public Internet	Training security awareness for users and employees about risks and threats on the public Internet

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: IAP301 ______________________________

Student Name: Nguyễn Quốc Vương ______________________________

Instructor Name: ______________________________

Lab Due Date: ______________________________

Overview

In this lab, you are to create an organization-wide Remote Access Policy for a mock organization under a recent compliance law. Here is your scenario:

- Regional ABC Healthcare Provider with multiple remote, healthcare branches and locations throughout the region
- Online access to patients' medical records through the public Internet is required for remote nurses and hospices providing in-home medical services
- Online access to patients' medical records from remote clinics is done through SSL VPN secure web application front-end through the public Internet
- The organization wants to be in compliance with HIPAA and IT security best practices regarding remote access through the public Internet in the Remote Access Domain
- The organization wants to monitor and control the use of remote access by implementing system logging and VPN connections
- The organization wants to implement a security awareness & training policy mandating that all new hires and existing employees obtain remote access security training. Policy definition to include HIPAA and ePHI (electronic personal healthcare information) security requirements and a mandate for annual security awareness training for all remote or mobile employees

Instructions

Using Microsoft Word, create a Remote Access Policy Definition capturing the elements of the policy as defined in the Lab #6 – Assessment Worksheet. Use the following policy template for the creation of your Remote Access Policy definition for a regional healthcare provider with remote medical clinics.

ABC Healthcare Provider

Remote Access Policy for Remote Workers & Medical Clinics

Policy Statement

Remote access policy is a document which outline and defines acceptable methods of remotely connecting to the internal network. It is essential in large organization where networks are geographically dispersed and extend into insecure network locations such as public networks or unmanaged home networks

{Insert policy verbiage here}

Purpose/Objectives

The objectives of a remote access policy to keep corporate data safe from exposure to hacker, malware,and other cybersecurity risks while allowing employees to work from remote location

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

This policy applies to all staff that access, configure, manage, and support remote connectivity to thenetwork

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?}

Standards

Remote Access Standard is to establish authorized method for remotely accessing resources and services securely

{Does this policy point to any hardware, software, or configuration standards? If so, list them here, and explain the relationship of this policy to these standards. In this case, Remote Access Domain standards should be referenced such as encryption standards, SSL VPN standards, – make any necessary assumptions.}

Procedures

Staff shall contact the help desk for approved methods and software to remotely connect to system; Staff accessing systems remotely are responsible for ensuring their mobile device is compliant with applicable policy; All devices shall be inspected be the help desk prior to use to ensure the device is up to date with all applicable security patches and virus malware

{Explain how you intend to implement this policy organization-wide and how you intend to deliver the annual or on-going security awareness training for remote workers and mobile employees.}

Guidelines

Data and network encryption standards Information security and confidentiality Email usagePhysical and virtual device security Network connectivityVPN access

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: ______________________________

Lab Due Date: ______________________________

Overview

This lab presents the risks and threats commonly found in the Remote Access Domain and how the use of the public Internet introduces new challenges regarding security and compliance for organizations. The students created a Remote Access Policy definition specific to a healthcare organization requiring remote access to patients' medical records systems from remote clinics and patient homes from mobile nurses and healthcare providers in the field.

Lab Assessment Questions & Answers

1. What are the biggest risks when using the public Internet as a WAN or transport for remote access to your organization's IT infrastructure?

   The problems or risk when using a WIFI is that, hackers often have the ability to position themselves between the user and the end point connection. And once these hackers gains access to your information and privacy

2. Why does this mock healthcare organization need to define a Remote Access Policy to properly implement remote access through the public Internet?

Because VPN is necessary when users want to access resource of organization through public internet

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?

The acceptable use policy is a component of the security awareness and training policy. This component specifies what user can and cannot do on company resources while the security awareness and training policy specifies security as a whole throughout the organization

4. One of the major prerequisites for this scenario was the requirement to support nurses and healthcare professionals that are mobile and who visit patients in their homes. Another requirement was for remote clinics to access a shared patient medical records system via a web browser. Which type of secure remote VPN solution is recommended for these two types of remote access?

For nurses and healthcare professionals, we use Remote Access VPN. Other is Site-to-Site VPN

5. When trying to combat unauthorized access and login attempts to IT systems and applications, what is needed within the LAN-to-WAN Domain to monitor and alarm on unauthorized login attempts to the organization's IT infrastructure?

Using Router to monitor and firewall to detected, alarm to Administrator

6. Why is it important to mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet?

Their ID and password can be leak when they try to login into the Remote Access

7. Why should social engineering be included in security awareness training?

Because it helps to defend against Sophisticated Phishing Attacks. Educate and Train your employees to prevent a socially engineering attack

8. Which domain (not the Remote Access Domain) throughout the seven domains of a typical IT infrastructure supports remote access connectivity for users and mobile workers needing to connect to the organization's IT infrastructure?

WAN Domain

9. Where are the implementation instructions defined in a Remote Access Policy definition? Does this section describe how to support the two different remote access users and requirements as described in this scenario?

The implementation instruction are defined in Remote Access Domain

10. A remote clinic has a requirement to upload ePHI data from the clinic to the organization's IT infrastructure on a daily basis in a batch-processing format. How should this remote access requirement be handled within or outside of this Remote Access Policy definition?

Remote access requirement should be handled to authorized member of the company and withthe use of active directory other users can use the VPN user access

11. Why is a remote access policy definition a best practice for handling remote employees and authorized users that require remote access from home or on business trips?

Remote access policy is best practice for handling remote employees and authorized users as it gives the user the security and flexible way to access network from anywhere

12. Why is it a best practice of a remote access policy definition to require employees and users to fill in a separate VPN remote access authorization form?

It is best practice of a remote access policy as it makes sure there are no repudiation of the user sothat only authorized person can access the important documents

13. Why is it important to align standards, procedures, and guidelines for a remote access policy definition?

It is important to align standards, procedures, and guidelines for a remote access policy for the data remains confidential as required by the law

14. What security controls, monitoring, and logging should be enabled for remote VPN access and users?

The security controls, monitoring, and logging should be enabled for remote VPN access and users are multifactor authentication of users, to monitor there is an account and computer audit policy and for logging event administrators will send access request or notification

15. Should an organization mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition?

I think yes, an organization should mention that it will be monitoring and logging remote access use in its remote access policy so that the organization will ensure transparency so that the employee will know the policy