Laboratory #5

Lab #5: Craft an Organization-Wide Security Awareness Policy

Learning Objectives and Outcomes

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

- Relate how risks, threats, and software vulnerabilities impact the seven domains of a typical IT infrastructure
- Identify the risks and threats commonly found within the User Domain and Workstation Domain
- Mitigate the risks and threats identified in the User Domain and Workstation Domain by incorporating these topics in the organization's security awareness training program
- Identify the key elements of a security awareness training policy as part of an overall layered security strategy
- Create an organization-wide security awareness training policy mandating annual or periodic security awareness training for new and existing employees

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 #5:

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 #5 – Student Steps:

The following are the steps that the student must follow as part of Lab #5 – Create an Organization-Wide Security Awareness Policy:

1. Review with the class examples of security awareness & training policies found on the Internet:
   Healthcare: State of North Carolina Department of Health & Human Services
   http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/06security_training_and_awareness.pdf

Higher-Education: University of Massachusetts

http://www.massachusetts.edu/policyfaq/faq.cfm

U.S. Federal Government: Department of Defense Information Assurance Awareness

http://iase.disa.mil/eta/iaav9/iaa_v9/index.htm

Healthcare: Community Health Care of Washington

http://chpw.org/assets/file/Security-Awareness-and-Training-Policy.pdf

2. Discuss what the risks and threats are within the User Domain per the bulleted list provided:
    - Dealing with humans and human nature
    - User or employee apathy towards information systems security policy
    - Accessing the Internet is like opening "Pandora's box."
    - Surfing the web can be a dangerous trek in unknown territory
    - Opening e-mails and unknown e-mail attachments can lead to malicious software and codes
    - Installing unauthorized applications, files, or data onto organization owned IT assets
    - Downloading applications or software with hidden malicious software or codes
    - Clicking on an unknown URL links with hidden scripts
3. Discuss what organizations can do to mitigate the risks and threats identified within the User Domain
4. Discuss what the risks and threats are within the Workstation Domain per the bulleted list provided:
    - Unauthorized access to workstation
    - Operating system software vulnerabilities
    - Application software vulnerabilities
    - Viruses, Trojans, worms, spyware, malicious software/code, etc.
    - User inserts CDs, DVDs, USB thumb drives with personal data and files onto organization-owned IT assets
    - User downloads unauthorized applications and software onto organization-owned IT assets
    - User installs unauthorized applications and software onto organization-owned IT assets
5. Discuss what organizations can do to mitigate the risks and threats identified within the Workstation Domain
6. Create the deliverables for Lab #5 – Assessment Worksheet

7. Answer the Lab #5 – Assessment Questions & Answers that must be submitted with this lab exercise

Deliverables

Upon completion of Lab #5: Create an Organization-Wide Security Awareness Policy, the students must provide the following deliverables as part of this lab:

1. Lab #5 – Security Awareness Training Policy Elements Assessment Worksheet
2. Lab #5 – Create a Security Awareness Training Policy Definition
3. Lab #5 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #5 that the student must conduct:

1. Was the student able to relate how risks, threats, and software vulnerabilities impact the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to identify risks and threats commonly found within the User Domain and Workstation Domain? – [**20%**]
3. Was the student able to mitigate the risks and threats identified in the User Domain and Workstation Domain by incorporating these topics in the organization's security awareness training program? – [**20%**]
4. Was the student able to identify the key elements of a security awareness training policy as part of an overall layered security strategy? – [**20%**]
5. Was the student able to create an organization-wide security awareness training policy mandating annual or periodic security awareness training for new and existing employees? – [**20%**]

Lab #5 – Assessment Worksheet

Elements of a Security Awareness & Training Policy

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: ______________________________

Lab Due Date: 9/11/2024

Overview

For each of the identified risks and threats within the User Domain and Workstation Domain, identify a security control or security countermeasure that can help mitigate the risk or threat.

User Domain Risks & Threats	Risk Mitigation Tactic/Solution
Dealing with humans and human nature	Automated Process
User or employee apathy towards information systems security policy	Require users and employees to takesecurity awareness training courses
Accessing the Internet is like opening "Pandora's box" given the threat from attackers	Restrict websites that users can access
Surfing the web can be a dangerous trek in unknown territory	Do not click on malicious links from strangesources
Opening e-mails and unknown e-mail attachments can unleash malicious software and codes	Do not open e-mail from unknown orsuspicious sources

Workstation Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Installing unauthorized applications, files, or data on organization owned IT assets can be dangerous	Create a whitelist and a blacklist ofsoftwares that are allowed or prohibited
Downloading applications or software with hidden malicious software or codes	Always run virus scanner on downloadedfiles
Clicking on an unknown URL link with hidden scripts	Do not click on suspicious links
Unauthorized access to workstation	Enforce strong access control andauthentication
Operating system software vulnerabilities	Update OS regularly to avoid knownvulnerabilities
Application software vulnerabilities	Update softwares to the latest version orremove them
Viruses, Trojans, worms, spyware, malicious software/code, etc.	Always let antivirus programs running
User inserts CDs, DVDs, USB thumb drives with personal files onto organization-owned IT assets	Restrict users from inserting personaldevices into organization-owned IT assets
User downloads unauthorized applications and software onto organization-owned IT assets	Create a whitelist and a blacklist ofsoftwares that are allowed or prohibited
User installs unauthorized applications and software onto organization-owned IT assets	Create a whitelist and a blacklist ofsoftwares that are allowed or prohibited

Lab #5 – Assessment Worksheet

Craft an Organization-Wide Security Awareness & Training Policy

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: ______________________

Lab Due Date: ______________________

Overview

In this lab, you are to create an organization-wide security awareness & training policy for a mock organization to reflect the demands of a recent compliance law. 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 in the User Domain and Workstation Domain
- 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
- Organization wants to implement the security awareness & training policy mandated for all new hires and existing employees. Policy definition to include GLBA and customer privacy data requirements and mandate annual security awareness training for all employees

Instructions

Using Microsoft Word, create a Security Awareness & Training Policy for ABC Credit union/bank capturing the elements of the policy as defined in the Lab #5 – Assessment Worksheet. Use the following policy template for the creation of your Security Awareness & Training Policy definition.

ABC Credit Union

Security Awareness & Training Policy

Policy Statement

{Insert policy verbiage here}

This policy establishes guidelines and procedures for security awareness and training at ABC Credit Union. It ensures compliance with the Gramm-Leach-Bliley Act (GLBA), IT security best practices, and the protection of customer privacy data. All employees, contractors, and third-party vendors must adhere to this policy

Purpose/Objectives

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

This policy ensures employee awareness of information security and customer privacy responsibilities. Objectives include GLBA compliance, protecting customer data, implementing content filtering, prohibiting personal use of IT assets, email security controls, and mandating annual security awareness training

Scope

{Define whom this policy covers and its scope.

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?}

This policy applies to all users with access to organization IT assets, covering GLBA compliance and customer privacy. It includes:Devices (computers, laptops, mobiles);Email and internet access; Customer dataNetworks, servers, and physical access

Standards

{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, Workstation Domain standards should be referenced – make any necessary assumptions.}

This policy mandates that all organization-owned workstations in the Workstation Domain follow standards for hardware, software, and configuration, including:Strong passwords and management tools; Regular OS and app updatesAntivirus software; Firewalls and network security; Encryption for sensitive data

Procedures

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

To enforce this policy, ABC Credit Union will:Provide annual security awareness training; Use content filtering to monitor Internet use; Prohibit personal use of IT assets; Implement email security controls

Guidelines

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

ABC Credit Union acknowledges potential challenges in implementing this policy and will:Provide clear communication and training on policy objectives; Inform employees of consequences for violations; Conduct regular audits to ensure compliance; Continuously update the policy to reflect changes in laws, regulations, and technology

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

Lab #5 – Assessment Worksheet

Craft an Organization-Wide Security Awareness & Training Policy

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: ______________________________

Lab Due Date: ______________________________

Overview

In this lab, the students reviewed and identified common risks and threats within the User Domain and Workstation Domain. From this, the elements of a security awareness training policy definition were aligned to policy definition goals and objectives. The students then created a Security Awareness & Training Policy definition focusing on the requirements as defined in the given scenario. This policy, coupled with actual security awareness training content customized to ABC Credit union/bank, can help mitigate the risks and threats within the User Domain and Workstation Domain and will contribute to the organization's overall layered security strategy.

Lab Assessment Questions & Answers

1. How does a security awareness & training policy impact an organization's ability to mitigate risks, threats, and vulnerabilities?

   A security awareness and training policy is essential for educating personnel on cybersecurity best practices, threat identification and response, and data protection, thereby reducing the risk of cyberattacks and data breaches

2. Why do you need a security awareness & training policy if you have new hires attend or participate in the organization's security awareness training program during new hire orientation?

Providing security awareness training to new hires during orientation is crucial. However, it is equally important to offer continuous training sessions that include updates on new threats and vulnerabilities. This approach keeps employees informed and prepared to identify and respond to potential risks effectively

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

An Acceptable Use Policy (AUP) and a Security Awareness & Training Policy are complementary. The AUP defines rules and guidelines for technology resource usage, while the Security Awareness & Training Policy educates employees on effectively adhering to these rules and guidelines

4. Why is it important to prevent users from engaging in downloading or installing applications and software found on the Internet?

Preventing users from downloading or installing software from the Internet is vital to protect the organization's security. Internet-sourced software may harbor malware and viruses that pose significant risks. By imposing restrictions, the organization mitigates potential security breaches and safeguards its assets

5. When trying to combat software vulnerabilities in the Workstation Domain, what is needed most to deal with operating system, application, and other software installations?

They need to ensure that all software installations, including operating systems and applications, receive regular security updates and patches

6. Why is it important to educate users about the risks, threats, and vulnerabilities found on the Internet and world wide web?

   Educating users about the risks, threats, and vulnerabilities found on the Internet and world wide web is necessary because it helps them understand why they need to remain vigilant and adopt safe browsing habits

7. What are some strategies for preventing users or employees from downloading ad installing rogue applications and software found on the Internet?

   Strategies for preventing users or employees from downloading and installing rogue applications and software found on the Internet include implementing permissions and access controls, whitelisting approved software, and regularly monitoring network traffic

8. What is one strategy for preventing users from clicking on unknown e-mail attachments and files?

   Training on how to detect phishing emails and suspicious attachments

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

   Because it is a common technique used by cybercriminals to trick users into divulging sensitive information or performing actions that could compromise an organization's security

10. Which 2 domains of a typical IT infrastructure are the focus of a Security Awareness & Training Policy?

The two domains of a typical IT infrastructure that are the focus of a Security Awareness & Training Policy are the User Domain and Workstation Domain

11. Why should you include organization-wide policies in employee security awareness training?

Organization-wide policies should be included in employee security awareness training because they help employees understand how their actions can impact the overall security posture of the organization.

12. Which domain typically acts as the point-of-entry into the IT infrastructure? Which domain typically acts as the point-of-entry into the IT infrastructure's systems, applications, databases?

The User Domain typically acts as the point-of-entry into the IT infrastructure, while the Workstation Domain typically acts as the point-of-entry into the IT infrastructure's systems, applications, and databases

13. Why does an organization need a policy on conducting security awareness training annually and periodically?

An organization needs a policy on conducting security awareness training annually and periodically to ensure that all personnel receive ongoing education on cybersecurity best practices and remain up-to-date with the latest threats and vulnerabilities

14. What other strategies can organizations implement to keep security awareness top of mind with all employees and authorized users?

Providing regular reminders and updates on security policies and procedures, using posters and other visual aids to reinforce key messages, and creating a culture of security where everyone takes responsibility for protecting sensitive information

15. Why should an organization provide updated security awareness training when a new policy is implemented throughout the User Domain or Workstation Domain?

Support employees understand any changes to policies and procedures and how to adhere to them effectively.