Laboratory #1

Lab #1: Craft an Organization-Wide Security Management Policy for Acceptable Use

Learning Objectives and Outcomes

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

- Define the scope of an acceptable use policy as it relates to the User Domain
- Identify the key elements of acceptable use within an organization as part of an overall security management framework
- Align an acceptable use policy with the organization's goals for compliance
- Mitigate the common risks and threats caused by users within the User Domain with the implementation of an acceptable use policy (AUP)
- Draft an acceptable use policy (AUP) in accordance with the policy framework 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 #1:

1. Standard onsite student workstation must have loaded the following software applications and access to the Internet to complete this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #1 – Student Steps

The following student steps are required to perform Lab #1: Create an Organization-Wide Security Management Policy for Acceptable Use:

1. Logon to your classroom workstation
2. Discuss the risks and threats within the User Domain
3. Discuss what organizations can do to mitigate the risks and threats identified within the User Domain. Explore issues related to the following circumstances:

- User apathy towards policies
- User inserts a CD or USB hard drive into the organization's workstation
- User downloads music, video, or other hidden malicious software or code
- User loses productivity by surfing the web
- User destruction or deletion of sensitive files and data
- Disgruntled employee
- Office romance "gone bad"
- Employee blackmail or extortion

4. Open your Internet Explorer web browser, and go to the following web sites:
   - Healthcare: http://it.jhu.edu/policies/itpolicies.html
   - Higher-Education: http://policies.georgetown.edu/31641.html
   - Banking: https://www.casecu.org/webfederal.asp?Cabinet=Home&Drawer=Main&Folder=MORTGAGE&SubFolder=Acceptable+Use+Policy&page_name=acceptable_use_policy
   - U.S. Federal Government: https://www.jointservicessupport.org/AUP.aspx
5. Review the key elements and scope of these sample acceptable use policies
6. Discuss how a risk can be mitigated within the User Domain with an acceptable use policy (AUP)
7. Review the Lab #1 scenario for the creation of an organization-wide security management policy for acceptable use
8. Conduct Lab #1: Craft an Organization-Wide Security Management Policy for Acceptable Use and Lab #1 – Assessment Questions & Answers

Deliverables

Upon completion of Lab #1: Create an Organization-Wide Security Management Policy for Acceptable Use, the students are required to provide the following deliverables:

1. Lab #1 – Craft an Organization-Wide Acceptable Use Policy (AUP)
2. Lab #1 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #1 that the students must perform:

1. Was the student able to define the scope of an acceptable use policy as it relates to the User Domain? – [**20%**]

2. Was the student able to identify key elements of acceptable use within an organization as part of an overall security management framework? – [**20%**]
3. Was the student able to align an acceptable use policy with the organization's goals for compliance? – [**20%**]
4. Was the student able to mitigate common risks and threats caused by users within the User Domain with the implementation of an acceptable use policy (AUP)? – [**20%**]
5. Was the student able to create an acceptable use policy in accordance with the policy framework definition that incorporates a policy statement, standards, procedures, and guidelines? – [**20%**]

Lab #1 – Organization-Wide Security Management AUP Worksheet

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you are to create an organization-wide acceptable use policy (AUP) that follows a recent compliance law for a mock organization. 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 its 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 implement this policy for all the IT assets it owns and to incorporate this policy review into an annual security awareness training

Instructions

Using Microsoft Word, create an Acceptable Use Policy for ABC Credit union/bank according to the following policy template:

ABC Credit Union

Policy Name

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

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

Scope

{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

{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.}

Procedures

[In this section, explain how you intend to implement this policy throughout this organization.}

Guidelines

[In this section, explain any road blocks or implementation issues that you must overcome and how you will overcome them per the defined policy guidelines.}

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

Lab #1 – Assessment Worksheet

Craft an Organization-Wide Security Management Policy for Acceptable Use

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, Create an Organization-Wide Security Management Acceptable Use Policy (AUP), the students participated in a classroom discussion about what is considered to be "acceptable use." The weakest link in the seven domains of a typical IT infrastructure was identified as the User Domain. When given a scenario, the students created an organization-wide acceptable use policy for ABC Credit Union/Bank.

Lab Assessment Questions & Answers

1. What are the top risks and threats from the User Domain?

2. Why do organizations have acceptable use policies (AUPs)?

3. Can internet use and e-mail use policies be covered in an Acceptable Use Policy?

4. Do compliance laws such as HIPPA or GLBA play a role in AUP definition?

5. Why is an acceptable use policy not a failsafe means of mitigating risks and threats within the User Domain?

6. Will the AUP apply to all levels of the organization, why or why not?

7. When should this policy be implemented and how?

8. Why does an organization want to align its policies with the existing compliance requirements?

9. Why is it important to flag any existing standards (hardware, software, configuration, etc.) from an AUP?

10. Where in the policy definition do you define how to implement this policy within your organization?

11. Why must an organization have an Acceptable Use Policy (AUP) even for non-employees such as contractors, consultants, and other 3rd parties?

12. What security controls can be deployed to monitor and mitigate users from accessing external websites that are potentially in violation of an AUP?

13. What security controls can be deployed to monitor and mitigate users from accessing external webmail systems and services (i.e., Hotmail, Gmail, Yahoo, etc.)?

14. What security controls can be deployed to monitor and mitigate users from imbedding privacy data in e-mail messages and/or attaching documents that may contain privacy data?

15. Should an organization terminate the employment of an employee if he/she violates an AUP?