Lab - Develop Cybersecurity Policies and Procedures

Introduction

Information security policies provide a framework for organizations to manage and protect their assets, and a safeguard that the organizations employ to reduce risk. Students will be required to compare information security policies to determine the differences between policies, standards, guidelines, and procedures. Students will then develop an information security policy to address existing vulnerabilities identified by an internal audit.

For example, a password policy states the standard for creating strong passwords and protecting passwords. A password construction guideline defines how to create a strong password and provides best practices recommendations. The password procedure provides the instructions on how to implement the strong password requirement. Organizations do not update policies as frequently as they update procedures within the information security policy framework.

Objectives

This project includes the following objectives:

Part 1: Review the Scenario

Part 2: Review and Prioritize Audit Findings

Part 3: Develop Policy Documents

Part 4: Develop a Plan to Disseminate and Evaluate Policies

Requirements

You will need internet access to the following websites, video, and documents:

- SANS Security Policy Project
  https://www.sans.org/security-resources/policies/
- Information Security Policy (video)
  https://youtu.be/ZlKgMUOpMf8
- Top Computer Security Vulnerabilities
  https://www.n-able.com/features/computer-security-vulnerabilities
- Information Security Policy – A Development Guide for Large and Small Companies (pdf)
  https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331
- Technical Writing for IT Security Policies in Five Easy Steps
  https://www.sans.org/reading-room/whitepapers/policyissues/technical-writing-security-policies-easy-steps-492

Scenario

ACME Healthcare is a healthcare company that runs over 25 medical facilities including patient care, diagnostics, outpatient care, and emergency care. The organization has experienced several data breaches over the last five years. These data breaches have cost the organization financially and damaged its reputation.

The executive leadership team recently hired a new chief information security officer (CISO). The new CISO has brought in one of the top cybersecurity penetration teams to perform a full security audit on the entire organization. This independent contractor conducted the audit, and found the following vulnerabilities:

1) Several accounts were identified for employees that are no longer employed by ACME.

2) Several user accounts allowed unauthorized and escalated privileges. These accounts accessed systems and information without formal authorization.
3) Several devices and systems allowed unsecure remote access.
4) Forty percent of all organization passwords audited were cracked within 6 hours.
5) Password expiration was not standardized.
6) Sensitive files were found unencrypted on user devices.
7) Several wireless hotspots used WEP for encryption and authentication.
8) Evidence indicates that sensitive e-mail was sent to and from employee homes and mobile devices without encryption.
9) Intrusion detection logs were infrequently reviewed and analyzed.
10) Devices with sensitive company data were used by employees for private use.
11) Employee devices were left unattended and employees failed to logout of the company network and data systems.
12) Inconsistent device updates and configurations were performed.
13) Several firewall rules were set to permit all traffic unless specifically denied.
14) Company servers were not updated with the latest patches.
15) The intranet web server allowed users to change personal information about themselves, including contact information.

Instructions

Part 1: Review of the Scenario

Read the scenario given above. Watch the Information Security Policy video. Take notes to help you differentiate the various levels and types of policies.

Part 2: Review and Prioritize Audit Findings

a. Research the types of vulnerabilities listed to determine which of them pose the greatest threat. Go to Top Computer Security Vulnerabilities to learn more.

b. Based on your research, list the top five security audit findings that ACME should address, starting with the greatest vulnerability.

c. Record your rankings in a **Vulnerabilities Ranking Table,** like the one shown below. It lists the *Vulnerabilities*, the *Recommended Policy* to mitigate this vulnerability, and your *Justification* for the ranking you determined.

Vulnerabilities Ranking Table		
Vulnerability	**Recommended Policy**	**Justification**
Forty percent of organization passwords were cracked within 6 hours.	**Password Management Policy**: Implement multi-factor authentication (MFA), use longer and more complex passphrases, prohibit password reuse, and educate users on password security.	Weak passwords expose the organization to brute-force attacks, leading to unauthorized access to critical systems. Implementing MFA significantly reduces the likelihood of unauthorized access.
Accounts belonging to former employees were still active.	**Account Management Policy**: Immediately disable or delete user accounts upon termination. Ensure access is revoked	Keeping former employee accounts active presents a major insider threat, as these accounts can be used to access

	across all internal systems.	sensitive data and systems without authorization.
Devices and systems allowed insecure remote access.	**Remote Access Policy**: Disable insecure remote access, implement VPN or SSH protocols for all remote connections.	Insecure remote access opens the door to cyberattacks and data breaches. Plaintext transmissions can be intercepted, exposing sensitive credentials and data to malicious actors.
Wireless hotspots used WEP for encryption and authentication.	**Wireless Network Security Policy**: Upgrade from WEP to WPA3 or other secure encryption protocols.	WEP is outdated and easily cracked, making wireless networks vulnerable to man-in-the-middle attacks and other breaches.
Company servers were not updated with the latest patches.	**System Maintenance Policy**: Implement regular patching for all servers and software, automate updates where possible.	Servers that are not updated with the latest security patches are vulnerable to well-known exploits, increasing the risk of data breaches and security incidents.

Blank Line, No additional information

Click **Show Answer** to a sample answer table.

Vulnerabilities Ranking Table		
Vulnerability	**Recommended Policy**	**Justification**
Several accounts were identified for employees that are no longer employed by ACME.	When an employee leaves the company: Review all access permission Retrieve data from the employee if appropriate Terminate access and reset all passwords	The former employee may gain unauthorized access to proprietary and confidential information and equipment. Anyone with the former employee's credentials can gain unauthorized access to internal system.
Several user accounts allowed unauthorized and escalated privileges and accessed systems and information without formal authorization.	Assign the least privilege to perform the task Log when elevated privileges are used	The least privilege allows the user to perform all the necessary tasks without the risk of causing systemic changes unintentionally.
Several devices and systems allowed unsecure remote access.	Disable unsecured remote access, such as Telnet Require secure remote access, such as SSH and VPN	Unsecured remote access transmits the data in plaintext. The transmission of plaintext can expose sensitive information, such as user credentials, for malicious actors to conduct reconnaissance and attacks.
Forty percent of all organization passwords audited were cracked within 6 hours.	New password policy: Implement 2FA or MFA User passphrases Change passwords only after evidence of compromise No reuse of old passwords No reuse of passwords on different applications Enable copy/paste passwords Educate users on basic cybersecurity	When the passwords are cracked, the attacker can gain unauthorized access and change the passwords to lock out the authorized users.
Several wireless hotspots used WEP for encryption and authentication.	Upgrade wireless hotspots to the most secure encryption and authentication available	WEP is prone to man-in-the-middle attacks and the key is easily cracked and hard to distribute to the users.
Company servers were not updated with the latest patches.	Establish a plan to update / test the latest patches at regular intervals.	Updating regularly can protect the data, fix security vulnerability, and improve the stability of the OS and applications.

Blank Line, No additional information

Part 3: Develop Policy Documents

Step 1: Create an Information Security Policy

a. Choose one vulnerability in the table for which to develop a security policy.

b. Use the Information Security Policy Templates to develop a specific security policy for ACME Healthcare that addresses your chosen vulnerability.

Note: Follow the template as a guideline. Address all existing policy elements. No policy should exceed two pages in length.

Step 2: Create a Procedure

a. Create a step-by-step set of instructions that supports your information security policy. Go to Information Security Policy — A Development Guide and Technical Writing for IT Security Policies in Five Easy Steps for instructions and guidance.

Note: All the above links will also be useful in Part 4 of this lab. Keep them open and bookmark them.

b. Include all the information that a user would need to properly configure or complete the task in accordance with the security policy.

Part 4: Develop a Plan to Disseminate and Evaluate Policies

Step 1: Create an Information Security Policy Implementation and Dissemination Plan.

a. Document the information required to create an information security policy implementation and dissemination plan.

b. Include specific tasks and events that ACME Healthcare will use to make sure that all employees involved are aware of the information security policies that pertain to them.

c. Include any specific departments that need to be involved. ACME Healthcare must also be able to assess whether individuals have the proper knowledge of the policies that pertain to their job responsibilities.

Conclusion

Information security policies provide a framework for how an organization protects its assets and is a safeguard that the organization employs to reduce risk. This project examined **why** an organization develops information security policies, and the **differences** between information security policies, standards, guidelines, and procedures. This project also explored how an organization disseminates and evaluates information security policies.

End of document