Nama : Wiraswanti Rismanda Putri

No : 20

Kelas : SIB-4C

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/securityresources/policies/
- Information Security Policy (video) https://youtu.be/ZlKgMUOpMf8
- Top Computer Security Vulnerabilities https://www.n-able.com/features/computer-securityvulnerabilities
- Information Security Policy – A Development Guide for Large and Small Companies (pdf) https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policydevelopmentguide-large-small-companies-1331
- Technical Writing for IT Security Policies in Five Easy Steps https://www.sans.org/readingroom/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**
Multiple accounts identified for employees who no longer work at ACME	When the employee is no longer with the company, a review of all access permissions should be done as well as terminating the access and resetting all passwords.	Former employees will have unauthorized access to private and confidential information and equipment.

Some user accounts allow unauthorized and elevated privileges and access to systems and information without formal authorization.	Assign privileges according to position	The lowest privilege allows users to perform necessary tasks without risk.
Some devices and systems allow insecure remote access.	Disable remote access and use SSH or VPN for secure remote access.	Insecure remote access sends data in the form of text that can reveal sensitive information and can be used by criminals to conduct surveillance and attacks.
Forty percent of all audited organizations' passwords were cracked within 6 hours.	Create a new password policy. Such as implementing 2FA or MFA, no old passwords, and educating users about cybersecurity.	If the password is successfully obtained, hackers can gain unauthorized access rights and change the password to lock out legitimate users.
Some wireless hotspots use WEP for encryption and authentication.	Upgrading wireless hotspots to be the most secure encryption and authentication	WEP is vulnerable to man-in-the-middle attacks and the keys are easy to crack and difficult to distribute to users

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.

Answer: Suppose the table contains a vulnerability such as “Weak and easily guessed passwords”. We will select this vulnerability as the focus of the security policy.

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

Answer:

- All users must use a strong password to access ACME Healthcare systems.
- Passwords must be updated every 90 days.
- Passwords should not be repeated within the last 12 cycles.
- Users are prohibited from using easily guessed personal information, such as name, date of birth, or surname as part of the password.
- The system will lock the user account after 5 consecutive failed login attempts to prevent brute force attacks.

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.

Answer:

The following are the procedures that support ACME Healthcare's Use of Strong Passwords policy:

Strong Password Configuration Procedure

1. Login to Security System
2. Navigate to Password Settings
3. Configure Password Policy
4. Set Automatic Account Lockout

5. Policy Testing
6. Provide User Guidance
7. Policy Monitoring and Enforcement

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

Answer:

To ensure users can follow this policy correctly, they need to be given additional instructions: 1. How to Create a Strong Password: ○ Create a password with at least 12 characters that includes a combination of uppercase, lowercase letters, numbers, and symbols.

- Avoid using personal information, such as names, dates of birth, or phone numbers.

2. Steps if Forgotten Password or Locked Account: ○ If you forget your password, use the Forgot Password feature on the login page to reset your password.
   - If your account is locked after 5 login attempts, contact IT to unlock your account.
3. Password Change: ○ Change your password every 90 days via profile settings.

By following the above procedures, a strong password security policy can be consistently implemented and maintained at ACME Healthcare.

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.

Answer:

Information Security Policy Implementation and Deployment Plan for ACME Healthcare:

1. **Implementation Objective:**
   - Ensure that the information security policy, specifically regarding the use of strong passwords, is understood and implemented by all ACME Healthcare employees.
   - Enhance protection of sensitive data and reduce the risk of unauthorized access.
2. **Implementation Target:**
   - All employees, contractors, and third parties with access to the company's information systems.
   - IT systems and applications used by ACME Healthcare.
3. **Required Resources:**
   - An IT team responsible for technical configuration of the system. ○ Training systems and educational materials for employees.
   - Audit tools to ensure policy compliance.
4. **Required Tools and Technology:**
   - Identity Access Management (IAM) system. ○ Automated password policy management system.

- Account lockout and audit system to prevent and track policy violations.

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.

   Answer:

   1. **Security Policy Training and Workshops:** Conduct information security training for all employees, including a guide on creating strong passwords, accessing systems, and steps to follow if an account is locked.
   2. **Distribution of Security Policy Materials:** Distribute policy guides in digital and print format to all employees via email, the company's intranet, and posters around the workplace.
   3. **Periodic Refresher Sessions:** Hold refresher sessions every 6 months to ensure employees remain compliant and understand the policy.
   4. **Compliance Audits and Assessments:** Conduct internal audits to ensure all employees adhere to the password policy.

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.

   Answer: IT Department, Information Security Department, HR Department, Management and Executive, Legal Department

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.