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 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

TASK 1

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.

****ANSWER****

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.
Forty percent of all organization passwords audited were cracked within 6 hours.	New password policy: Implement 2FA or MFA Change passwords only after evidence of compromise No reuse of old passwords No reuse of passwords on different applications	When the passwords are cracked, the attacker can gain unauthorized access and change the passwords to lock out the authorized users.
Sensitive files were found unencrypted on user devices.	All sensitive files should be encrypted while being processed and stored as well.	Sensitive files are more prone to attacks like unauthorized access because it contains sensitive information.
Devices with sensitive company data were used by employees for private use.	Company devices that store or access sensitive company data must not be used for personal or private activities by employees.	Using company devices for personal use increases the risk of data breaches, malware infections, and unauthorized data access.

TASK 2

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.

ANSWER

Vulnerability:

Forty percent of all organization passwords audited were cracked within 6 hours.

Password Security Policy

1. Purpose

   This policy defines the minimum password requirements and standards to ensure secure user authentication and protect sensitive ACME Healthcare data from unauthorized access.

2. Scope

   This policy applies to all employees, contractors, consultants, temporary staff, and third-party personnel who have access to ACME Healthcare's systems, networks, and data.

3. Policy

   - All passwords must contain a minimum of 16 characters.
   - Passwords must include a mix of upper and lower-case letters**,** numbers, and special characters**.**
   - Users are encouraged to use passphrases (e.g., "Coffee@6amIsBest!" or "sun-hike-breeze-trees").
   - Passwords must not be reused across different applications or platforms.
   - Old passwords must not be reused.
   - Password changes are required only when there is evidence or suspicion of compromise.
   - Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) is required wherever supported

4. Policy Sanctions

   Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities.

****TASK 3****

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.

****ANSWER****

Procedure

Step-by-Step Instructions

1. Creating a Secure Password

When setting or updating a password:

- Ensure your password is at least 16 characters long.
- Include a mix of the following:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0–9)
  - Special characters (e.g., !@#$%^&*)
- Recommended: Use a memorable passphrase.
  Example: "Coffee@6amIsBest!" or "sun-hike-breeze-trees"

2. Avoid Common Mistakes

- Do not reuse the same password across different systems (e.g., using your email password for HR software).
- Do not reuse old passwords when prompted to change.
- Avoid names, birthdates, or common phrases like "Password123!"
- Never write down your password or store it in unencrypted files.

3. Changing a Password

Only change your password if:

- You suspect compromise (e.g., you clicked on a suspicious email link).
- You are instructed by IT Security after a security scan.

- You are locked out due to failed login attempts.

To change your password:

1. Go to your account settings in the system.
2. Select “Change Password.”
3. Enter your current password.
4. Enter a new, compliant password.
5. Confirm the new password.
6. Save the changes.

4. Enable Two-Factor or Multi-Factor Authentication (2FA/MFA)

2FA/MFA is required wherever supported.

To enable MFA:

1. Go to Settings > Security in your application (e.g., email).
2. Select Enable 2FA/MFA.
3. Choose an authentication method:
   - Authenticator app (e.g., Google Authenticator)
   - SMS verification
4. Follow on-screen instructions to complete setup.
5. Save your backup codes in a secure location (not your email or notepad).

****TASK 4****

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.

****ANSWER****

Required Information for the Implementation Plan

- Policy version, purpose, and scope
- List of affected users (e.g., employees, contractors, third-party users)

- Key stakeholders and departments involved
- Communication channels for policy dissemination
- Training and awareness program details
- Timeline and milestones
- Process for feedback and continuous improvement
- Policy review cycle and responsible team

Specific Events and Tasks

- Send official policy document to all employees via internal email
- Upload the policy to the intranet under the "Security Policies" section
- Conduct live or recorded training session on password best practices
- Require all staff to digitally acknowledge they have read and understood policy
- Notify and assist users who missed training or failed the quiz
- Display visual reminders in offices and break rooms
- Host support sessions to help users enable 2FA/MFA on all supported systems
- Conduct survey to gather feedback on clarity and effectiveness

Specific departments that need to be involved

- IT Security: Enforces the policy, manages MFA, and conducts audits.
- HR: Shares the policy, tracks training, and handles acknowledgments.
- Training Team: Delivers sessions and trainings.
- Compliance: Ensures legal and regulatory alignment.

To check understanding, ACME will use:

- Mandatory training and sessions
- Digital acknowledgment forms
- Random compliance checks
- Support sessions for MFA setup
- Feedback surveys to improve clarity

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.