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.

[Answer]

The scenario presents significant vulnerabilities at ACME Healthcare, requiring various policies, standards, guidelines, and procedures to mitigate them.

Review the types of cybersecurity documents:

- Policy : Broad, high-level document that outlines rules to achieve specific goals (e.g., password policy).
- Standards : Specific low-level mandatory controls to enforce policies (e.g., minimum password length).
- Guidelines : General recommendations that can be followed to meet policy objectives (e.g., creating strong passwords).
- Procedures : Step-by-step instructions for implementing policies and standards (e.g., how to update user accounts after termination).

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 user accounts allowed unauthorized and escalated privileges	Implement Access Control Policy	Privileged accounts can provide access to sensitive systems, potentially leading to data breaches and unauthorized changes. Assign least privilege for safety.
Forty percent of all organization passwords were cracked within 6 hours	Implement Password Policy with MFA and Passphrase Rules	Weak passwords are easily compromised. Using multi-factor authentication (MFA) and passphrases drastically reduces unauthorized access risks.
Several accounts identified for employees no longer employed by ACME	Develop Account Management Policy	Ex-employees having access can result in unauthorized data access or malicious actions. Timely account termination mitigates these risks.
Several devices and systems allowed unsecure remote access	Implement Remote Access Policy using secure protocols	Unencrypted remote access, such as Telnet, exposes sensitive data in transit. Use secure methods like SSH or VPN to mitigate man-in-the-middle attacks.

Vulnerabilities Ranking Table		
Several wireless hotspots used WEP for encryption and authentication	Establish Wireless Security Policy mandating WPA3	WEP encryption is outdated and vulnerable. Upgrading to WPA3 protects against common wireless attacks and improves overall network security.

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.

[Answer]

Step 1: Create an Information Security Policy

Chosen Vulnerability

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

Security Policy

ACME Healthcare Password Policy

Purpose

The purpose of this policy is to establish a standard for the creation, management, and protection of passwords at ACME Healthcare to ensure the security and confidentiality of sensitive information. This policy aims to reduce the risk of unauthorized access caused by weak passwords or password reuse.

Scope

This policy applies to all employees, contractors, and third-party users who access ACME Healthcare's systems and networks.

Policy

1. Password Requirements:
    - All user accounts must be protected by strong passwords.
    - Passwords must be a minimum of 12 characters and include a combination of uppercase letters, lowercase letters, numbers, and special characters.
    - Common passwords such as "password," "123456," or any variation of the user's name are prohibited.
    - Passphrases are encouraged for added security.
2. Password Expiration:
    - Passwords must be changed every 180 days or immediately upon suspected compromise.
    - Multi-factor authentication (MFA) must be enabled for access to sensitive systems.
3. Password Reuse:
    - Users are prohibited from reusing old passwords within the last 5 password cycles.
    - Passwords must not be reused across different platforms or applications.

4. Account Lockout:
    - Accounts will be locked after 5 failed login attempts. The account will remain locked until reset by an administrator.
5. Storage and Sharing
    - Passwords must never be written down or stored in unencrypted formats (e.g., text files).
    - Password sharing is strictly prohibited.
    - Employees must use password managers approved by the IT department to store and manage passwords securely.
6. Enforcement:
    - Violations of this policy will result in disciplinary action, which may include termination of employment.
    - IT administrators are responsible for ensuring all systems comply with these requirements.

Exceptions

Exceptions to this policy must be approved in writing by the Chief Information Security Officer (CISO).

Review and Revision

This policy will be reviewed annually by the Information Security team and updated as necessary to address emerging threats.

Step 2: Create a Procedure

Procedure:

Password Creation and Management Procedure

This procedure provides step-by-step instructions for creating and managing passwords in accordance with ACME Healthcare's Password Policy.

Purpose

To guide users on how to create, update, and securely manage passwords.

Scope

This procedure applies to all users who are required to set or reset passwords for ACME Healthcare systems.

Procedure:

Step 1: Creating a New Password

1. Open the login screen for the ACME Healthcare system.
2. When prompted to set a new password:
    - Enter a password that is at least 12 characters long.
    - Ensure the password contains:
        - At least one uppercase letter (A-Z).
        - At least one lowercase letter (a-z).
        - At least one number (0-9).
        - At least one special character (e.g., !, @, #, $, etc.).
    - Avoid using easily guessable information such as your name, birthdate, or simple patterns like "1234."
3. Confirm the password by typing it again.
4. Click "Submit" to save your new password.

Step 2: Using Multi-Factor Authentication (MFA)

1. Download and install the approved MFA application (e.g., Google Authenticator, Duo).
2. During your next login attempt:
    - Enter your password as usual.

- When prompted, open the MFA app and enter the code provided or approve the login request.

3. If you lose access to your MFA app, contact IT Support immediately to reset your access.

Step 3: Changing Your Password

1. Log in to the ACME Healthcare system.
2. Navigate to the account settings or password management section.
3. Click "Change Password."
4. Enter your current password for verification.
5. Create a new password following the guidelines:
   - At least 12 characters long.
   - Combination of uppercase letters, lowercase letters, numbers, and special characters.
6. Re-enter the new password to confirm.
7. Click "Save" to complete the password change.

Step 4: Handling Forgotten Passwords

1. On the login page, click "Forgot Password."
2. Enter your registered email address or username.
3. Check your email for a password reset link.
4. Follow the instructions in the email to create a new password using the guidelines provided.
5. If you do not receive a password reset email, contact IT Support.

Step 5: Storing Passwords Securely

1. Never store passwords in unencrypted text files or written notes.
2. Use the IT-approved password manager to store and manage passwords securely.
   - Open the password manager application.
   - Add a new entry by providing the name of the system and your password.
   - Ensure the password manager is locked when not in use.
3. Do not share your password with others. If assistance is needed, contact IT Support for secure password recovery options.

Step 6: Monitoring and Reporting

1. Regularly check your account activity for any unauthorized access.
2. Immediately report any suspected password compromise to the IT security team.
3. Participate in ongoing cybersecurity awareness training provided by the organization.

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]

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

Objective

The goal of this plan is to ensure that ACME Healthcare employees are fully aware of and comply with the new password policy, understand its importance, and can implement it properly. The plan will focus on the steps required to effectively communicate the new policy, train employees, and assess their compliance.

A. Key Components of the Plan

1. Policy Documentation:
    - The new Password Policy and supporting procedures will be documented and published in a centralized internal system accessible to all employees. This will include the policy document, password creation and management procedures, and guidelines on the use of multi-factor authentication (MFA).
2. Target Audience:
    - All ACME Healthcare employees who have access to the company's internal systems, including full-time, part-time, contractors, and third-party vendors.
    - Specific departments that need special focus include:
        - IT Department: Responsible for implementing technical measures such as password management tools, MFA, and account lockout settings.
        - HR Department: Responsible for integrating password policy training into onboarding and ongoing employee education.
        - Compliance and Audit Team: Responsible for ensuring that policies are properly followed and that regular audits are conducted.
3. Roles and Responsibilities:
    - Chief Information Security Officer (CISO): Oversees the implementation and dissemination of the policy.
    - IT Security Team: Responsible for technical implementation, including system configuration, MFA setup, and monitoring.
    - HR Department: Responsible for ensuring that all employees receive proper training on the new policy.
    - Department Heads: Responsible for ensuring their team members comply with the policy and report any issues or feedback.

B. Tasks and Events for Dissemination

1. Policy Announcement:
    - Objective: Communicate the importance and details of the new Password Policy to all employees.
    - Task:
        - A company-wide email from the CISO announcing the new policy, outlining the key points, and providing links to the full documentation and procedures.
        - Information sessions and webinars will be scheduled to explain the policy in detail.
    - Timeline: One week after the final policy approval.
    - Owner: CISO and IT Department.
2. Training Sessions:
    - Objective: Ensure employees understand how to comply with the new password requirements.
    - Task:
        - Conduct mandatory training sessions via the Learning Management System (LMS) for all employees on how to create strong passwords, use MFA, and manage their credentials.
        - Provide hands-on tutorials for the use of the approved password manager.
        - IT Department to conduct technical workshops for system administrators and power users to understand the MFA setup and account lockout settings.
    - Timeline: Training must be completed within 30 days of policy dissemination.
    - Owner: HR Department in collaboration with the IT Security Team.
3. Support Channels:
    - Objective: Provide employees with the support needed to implement the new policy.
    - Task:
        - Set up a helpdesk and FAQs specifically for password-related issues.
        - Create a dedicated email address for employees to ask questions or report problems during the transition.

        - IT team available for one-on-one assistance in setting up MFA and managing password managers.
    - Timeline: Ongoing during the implementation phase and beyond.
    - Owner: IT Support Team.
4. Reminders and Follow-ups:
    - Objective: Reinforce the importance of complying with the new policy and address any gaps in training or compliance.
    - Task:
        - Weekly reminders via email and internal communications (e.g., company intranet) to ensure employees are aware of upcoming deadlines for compliance.
        - Managers will follow up with their teams to confirm policy implementation.
    - Timeline: Begin two weeks after initial dissemination and continue for one month.
    - Owner: Department Heads and HR.

C. Evaluation and Compliance Assessment

1. Policy Compliance Monitoring:
    - Objective: Ensure that the policy is being adhered to by all employees.
    - Task:
        - IT Department will regularly monitor password compliance, including password strength, password reset cycles, and MFA adoption rates.
        - Automated systems will flag accounts that do not comply with the password requirements, triggering enforcement actions such as account lockout or notification to supervisors.
    - Timeline: Ongoing.
    - Owner: IT Department and Compliance Team.
2. Audits and Reviews:
    - Objective: Evaluate the effectiveness of the policy and its implementation.
    - Task:
        - Regular security audits will be conducted every quarter to ensure compliance with the password policy.
        - Conduct random password strength tests and identify any areas for improvement.
    - Timeline: Quarterly, starting 3 months after policy implementation.
    - Owner: Compliance and Audit Team.
3. Employee Knowledge Assessment:
    - Objective: Ensure that employees understand the policy and its relevance to their roles.
    - Task:
        - Use quizzes and assessments as part of the training sessions to gauge employee understanding of the password policy and best practices.
        - Performance reviews will include compliance with the policy as part of the evaluation.
    - Timeline: After completion of training and every year during the annual performance review.
    - Owner: HR Department.

D. Reporting and Feedback Mechanism

1. Objective: Continuously improve the policy based on feedback and changing threats.
2. Task:
    - Provide a feedback form for employees to report challenges or suggestions regarding the policy.
    - Regular feedback sessions with Department Heads and IT staff to address any implementation issues.
    - CISO to compile a quarterly report on policy effectiveness, including compliance rates, security incidents, and recommendations for improvements.
3. Timeline: Quarterly review and report generation.

4. Owner: CISO and HR.

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.