Nama : Yusufa Haidar

Kelas : SIB-3C

Absen : 21

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.

- Unsecure Password Practices (Findings 4 & 5)
- Unauthorized Access and Escalated Privileges (Findings 1 & 2)
- Unencrypted Sensitive Data (Findings 6 & 8)

- Unsecure Remote Access and Weak Wireless Security (Findings 3 & 7)
- Unpatched Servers and Devices (Findings 12 & 14)

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**
Unsecure Password Practices	Implement a strong password policy with mandatory complexity, regular expiration, and multi-factor authentication (MFA).	Weak passwords are an easy entry point for attackers, and enforcing stricter password rules reduces the likelihood of password-related breaches.
Unauthorized Access and Escalated Privileges	Enforce role-based access control (RBAC) and regularly audit accounts to remove or disable unused ones.	Limiting account privileges and deactivating inactive accounts reduces the risk of insider threats and unauthorized access to sensitive systems.
Unencrypted Sensitive Data	Enforce encryption for all sensitive data at rest and in transit, including files and emails.	Encryption protects data from unauthorized access, safeguarding the organization against breaches of sensitive information.
Unsecure Remote Access and Weak Wireless Security	Require secure remote access through VPNs and upgrade wireless networks to WPA3 encryption.	Securing remote access and improving wireless encryption prevents unauthorized external access, reducing the risk of remote attacks.
Unpatched Servers and Devices	Establish a patch management policy with regular updates for all servers and devices.	Regular updates mitigate vulnerabilities, preventing attackers from exploiting outdated software to gain access to systems.

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.

Vulnerabilities Ranking Table		
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.

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.

- Unsecure Password Practices

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.

- Define Password Complexity Requirements
  - Action: Update password policy settings in the organization's directory service or authentication system to enforce a minimum length of 12 characters, including a mix of uppercase and lowercase letters, numbers, and special characters.
  - Responsible Party: IT Security Team
  - Timeline: Within 1 week
- Implement Password Expiration Rules
  - Action: Configure password expiration settings to require users to change their passwords every 90 days. Set up automated reminders to notify users 14 days before their passwords expire.
  - Responsible Party: System Administrators
  - Timeline: Within 2 weeks
- Enforce Password History and Non-Reuse
  - Action: Adjust system settings to prevent users from reusing any of their last 5 passwords. Ensure this setting is applied to all user accounts.
  - Responsible Party: IT Support Team
  - Timeline: Within 1 week
- Enable Multi-Factor Authentication (MFA)
  - Action: Implement MFA for all critical systems and applications, including remote access points. Configure MFA to require a secondary verification method (e.g., SMS code, authentication app).
  - Responsible Party: IT Security Team
  - Timeline: Within 1 month
- Secure Password Storage
  - Action: Ensure that all passwords are stored using secure hashing and encryption methods. Avoid plain text storage. Review and update password storage mechanisms if necessary.
  - Responsible Party: Development Team / IT Security Team
  - Timeline: Within 2 weeks
- Implement Account Lockout Policy
  - Action: Configure systems to lock user accounts after 5 failed login attempts. Establish a process for account unlock requests, requiring administrative intervention.
  - Responsible Party: System Administrators
  - Timeline: Within 1 week
- Conduct Regular Policy Audits

        - Action: Schedule and perform annual audits to review compliance with the password management policy. Review password security settings, user adherence, and the effectiveness of the policy.
        - Responsible Party: IT Security Team
        - Timeline: Annually
    - Communicate and Train
        - Action: Inform all employees about the new password management policy through internal communication channels. Provide training sessions to ensure understanding and compliance.
        - Responsible Party: HR and IT Training Team
        - Timeline: Within 2 weeks

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.

- **Policy Details**
    - **Content**: Full text of the information security policies, including objectives, scope, and specific requirements.
    - **Reference**: Include links or documents that provide additional context or related policies.
- **Stakeholders**
    - **Identification**: List of departments and individuals who need to be involved in the implementation and dissemination.
    - **Roles**: Define specific roles and responsibilities for each stakeholder.
- **Training Materials**
    - **Content**: Development of training modules, presentations, and user guides that explain the policies and procedures.
    - **Format**: Choose delivery formats (e.g., online courses, in-person training) and ensure materials are accessible.
- **Communication Channels**
    - **Methods**: Determine how policies will be communicated (e.g., email, intranet announcements, team meetings).
    - **Frequency**: Set up regular communication updates and reminders.
- **Implementation Timeline**
    - **Schedule**: Create a timeline for policy rollout, including key milestones and deadlines.

- **Tasks**: Outline specific tasks to be completed and assign responsible parties.

- **Assessment and Monitoring**

  - **Methods**: Develop procedures for evaluating policy awareness and compliance.
  - **Tools**: Identify tools and methods for tracking adherence and conducting assessments.

- **Feedback Mechanism**

  - **Process**: Set up a system for employees to provide feedback and ask questions about the policies.
  - **Support**: Designate points of contact for policy-related inquiries and support.

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.

- **Initial Rollout**

  - **Task**: Distribute the full text of the new policies to all employees.
  - **Event**: Host a company-wide meeting or webinar to introduce the policies and highlight key points.

- **Departmental Briefings**

  - **Task**: Schedule briefings with each department to explain how the policies apply to their specific roles.
  - **Event**: Conduct departmental meetings or workshops with tailored presentations.

- **Training Sessions**

  - **Task**: Develop and conduct mandatory training sessions for all employees on the new policies.
  - **Event**: Organize online or in-person training sessions and track attendance and completion.

- **Policy Documentation**

  - **Task**: Post the policies on the company intranet and ensure they are easily accessible.
  - **Event**: Update the intranet with policy documents and provide a dedicated section for policy-related resources.

- **Regular Updates and Reminders**

  - **Task**: Send periodic email reminders about the policies and any updates or changes.
  - **Event**: Schedule quarterly or bi-annual email blasts or newsletters.

- **Knowledge Assessments**

  - **Task**: Conduct assessments or quizzes to evaluate employee understanding of the policies.
  - **Event**: Implement knowledge checks after training sessions and periodically to ensure ongoing compliance.

- **Feedback Collection**

    - **Task**: Set up a feedback system for employees to report issues or seek clarification about the policies.
    - **Event**: Regularly review feedback and address common questions or concerns.

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.

- **Human Resources (HR)**

    - **Role**: Oversee policy distribution, manage training schedules, and handle employee inquiries.
    - **Involvement**: Ensure all employees receive training and are aware of policy requirements.

- **IT Security Team**

    - **Role**: Develop, update, and implement the security policies; provide technical support for policy-related issues.
    - **Involvement**: Assist with training on technical aspects of the policies and implement security measures.

- **Legal Department**

    - **Role**: Review policies for compliance with legal and regulatory requirements.
    - **Involvement**: Ensure that policies meet legal standards and assist with any legal implications of policy changes.

- **Department Heads/Managers**

    - **Role**: Ensure their teams understand and comply with the policies.
    - **Involvement**: Facilitate departmental briefings, monitor policy adherence, and report compliance issues.

- **Training and Development Team**

    - **Role**: Create and deliver training materials and sessions.
    - **Involvement**: Develop educational content and organize training events.

- **Internal Audit Team**

    - **Role**: Assess policy compliance and effectiveness.
    - **Involvement**: Conduct audits, review policy adherence, and provide feedback for improvement.

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.