Name : Selly Amelia Putri (2141762142)
Class : SIB 4C (16)

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**
SQL injection	Implement prepared statements and input validation	SQL injection can provide unauthorized access to databases, potentially exposing or corrupting sensitive data.
OS command injection	Avoid using shell commands, use secure APIs instead	Allows attackers to execute malicious commands on the operating system, potentially taking over the entire system.
Missing authentication for critical function	Implement multi-factor authentication for critical functions	Without proper authentication, attackers can access and manipulate important system functions.
Cross-site scripting and forgery	Implement input validation and output encoding	Allows attackers to inject malicious scripts, potentially stealing user data or altering website functionality.
Missing data encryption	Implement end-to-end encryption for sensitive data	Unencrypted data is vulnerable to theft and misuse if accessed by unauthorized parties.

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.

Vulnerabilities Ranking Table		
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.

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.

Information Security Policy: SQL Injection Prevention

Policy Statement:

ACME Healthcare is committed to protecting its databases and sensitive information from unauthorized access and manipulation. This policy outlines the requirements for preventing SQL injection attacks.

Purpose:

To establish guidelines and practices that ensure the security of our database systems against SQL injection vulnerabilities.

Scope:

This policy applies to all employees, contractors, and third-party vendors who develop, maintain, or interact with ACME Healthcare's database systems.

Policy Elements:

1. Input Validation:
    - All user inputs must be validated before being used in SQL queries.
    - Input validation must check for proper data types, lengths, and formats.
    - Reject or sanitize any input containing SQL keywords or special characters.
2. Prepared Statements:
    - Use parameterized queries or prepared statements for all database interactions.
    - Avoid dynamic SQL construction using string concatenation.
3. Least Privilege:
    - Database accounts used by applications must have minimal necessary permissions.
    - Regularly review and audit database access permissions.
4. Error Handling:
    - Implement custom error pages to prevent disclosure of database information.
    - Log all SQL errors for review but do not display them to end-users.
5. Database Security:
    - Enable SQL Server security features such as SQL Server Audit.
    - Regularly apply security patches and updates to database systems.
6. Code Review:
    - Conduct regular code reviews focusing on database interaction points.
    - Use static code analysis tools to identify potential SQL injection vulnerabilities.
7. Training:
    - Provide annual security awareness training for all developers on SQL injection prevention.
8. Testing:
    - Perform regular penetration testing and vulnerability assessments on database systems.

Compliance:

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

Policy Review:

This policy will be reviewed annually and updated as necessary to reflect changes in technology and security best practices.

Procedure: Implementing Prepared Statements for SQL Injection Prevention

Purpose: To provide step-by-step instructions for developers to implement prepared statements in database queries to prevent SQL injection attacks.

Procedure Steps:

1. Identify Query Points:
    - Action: Review all database interaction points in the application.
    - Responsible Party: Development Team

- Timeline: Within 1 week

2. Refactor Queries:
   - Action: Replace dynamic SQL queries with prepared statements.
   - Responsible Party: Development Team
   - Timeline: Within 2 weeks
3. Implement Prepared Statements:
   - Action: Use the following pattern for all database queries:

```
using (SqlConnection connection = new
SqlConnection(connectionString))
{
    string query = "SELECT * FROM Users WHERE Username = @Username
AND Password = @Password";
    SqlCommand command = new SqlCommand(query, connection);
    command.Parameters.AddWithValue("@Username", username);
    command.Parameters.AddWithValue("@Password", password);

    connection.Open();
    SqlDataReader reader = command.ExecuteReader();
    // Process results
}
```

   - Responsible Party: Development Team
   - Timeline: Within 3 weeks
4. Input Validation:
   - Action: Implement input validation for all user inputs before using in queries.
   - Responsible Party: Development Team
   - Timeline: Within 2 weeks
5. Code Review:
   - Action: Conduct peer code reviews to ensure all queries use prepared statements.
   - Responsible Party: Senior Developers
   - Timeline: Ongoing, with initial review within 4 weeks
6. Testing:
   - Action: Perform thorough testing of refactored queries to ensure functionality.
   - Responsible Party: QA Team
   - Timeline: Within 1 week after development completion
7. Security Audit:
   - Action: Conduct a security audit of the database layer to verify proper implementation.
   - Responsible Party: IT Security Team
   - Timeline: Within 2 weeks after testing completion

8. Documentation:
    - Action: Update developer guidelines and coding standards to reflect the use of prepared statements.
    - Responsible Party: Technical Writing Team
    - Timeline: Within 1 week after security audit
9. Training:
    - Action: Provide training sessions on using prepared statements and SQL injection prevention.
    - Responsible Party: IT Training Team
    - Timeline: Within 2 weeks after documentation completion
10. Monitoring:
    - Action: Implement ongoing monitoring for SQL injection attempts and prepared statement usage.
    - Responsible Party: IT Security Team
    - Timeline: Continuous, starting immediately after implementation

By following this policy and procedure, ACME Healthcare will significantly reduce its vulnerability to SQL injection attacks, enhancing the security of its database systems and protecting sensitive patient information.

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.

Information Security Policy Implementation and Dissemination Plan

1. Policy Development and Approval

- Responsible Department: IT Security Team
- Tasks:
    - Draft policies addressing identified vulnerabilities
    - Review and refine policies with relevant stakeholders
    - Obtain executive approval for finalized policies

2. **Communication Strategy**
    - Responsible Department: HR and Internal Communications
    - Tasks:
        - Develop a communication plan for policy rollout
        - Create clear, concise summaries of each policy
        - Prepare FAQ documents to address common questions
3. **Training Program Development**
    - Responsible Department: IT Training Team
    - Tasks:
        - Design role-specific training modules
        - Develop interactive e-learning courses
        - Create hands-on workshops for critical policies
4. **Policy Dissemination**
    - Responsible Departments: HR, IT, and Department Managers
    - Tasks:
        - Distribute policies through company intranet and email
        - Conduct department-specific briefings
        - Include policy awareness in new employee onboarding
5. **Training Implementation**
    - Responsible Departments: IT Training and Department Managers
    - Tasks:
        - Schedule and conduct training sessions
        - Track attendance and completion rates
        - Provide ongoing support and resources
6. **Awareness Campaign**
    - Responsible Department: Marketing and Internal Communications
    - Tasks:
        - Create posters and digital signage for common areas
        - Develop a series of awareness emails and newsletters
        - Organize "Security Awareness Week" with special events
7. **Policy Compliance Monitoring**
    - Responsible Department: IT Security and Compliance Team
    - Tasks:
        - Implement automated policy compliance checks where possible
        - Conduct regular audits of policy adherence
        - Report compliance metrics to management

8. **Knowledge Assessment**
    - Responsible Departments: HR and IT Security
    - Tasks:
        - Develop role-specific quizzes to test policy knowledge
        - Implement annual policy comprehension assessments
        - Provide targeted retraining for areas of weakness
9. **Feedback Collection**
    - Responsible Departments: HR and IT Security
    - Tasks:
        - Set up an anonymous feedback system for policy concerns
        - Conduct periodic surveys on policy effectiveness
        - Hold focus groups to gather in-depth feedback
10. **Continuous Improvement**
    - Responsible Department: IT Security Team
    - Tasks:
        - Review feedback and assessment results quarterly
        - Update policies and training materials as needed
        - Report on policy effectiveness to executive leadership
11. **Integration with Performance Management**
    - Responsible Department: HR
    - Tasks:
        - Include policy compliance in annual performance reviews
        - Recognize and reward exemplary policy adherence
        - Address repeated non-compliance through disciplinary processes
12. **Vendor and Contractor Management**
    - Responsible Departments: Procurement and IT Security
    - Tasks:
        - Ensure relevant policies are communicated to external parties
        - Include policy compliance in vendor contracts
        - Conduct periodic audits of vendor adherence to policies

This plan ensures that ACME Healthcare systematically implements, disseminates, and evaluates its information security policies across all relevant departments. By involving multiple departments and incorporating various methods of communication, training, and assessment, the organization can effectively reduce security risks and foster a culture of security awareness among all employees.