Develop Cybersecurity Policies and Procedures

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 insecure 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 email 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**
Unauthorized and Escalated Privileges	**Least Privilege Policy** • Grant users only the permissions necessary to perform their job functions. • Implement regular reviews of user roles and privileges.	This allows unauthorized access to sensitive information and systems, increasing the risk of insider threats and data breaches.
Weak Password Security	**Password Policy** • Enforce strong password requirements (length, complexity). • Implement regular password changes and disallow reuse. • Use MFA to enhance account security.	40% of passwords cracked within 6 hours is alarmingly high. Weak passwords are a primary entry point for attackers.
Permissive Firewall Rules	**Firewall Configuration Policy** • Implement a deny-by-default rule, only permitting necessary traffic. • Regularly review and update firewall rules to reflect current needs.	Allowing all traffic unless specifically denied increases the risk of unauthorized access and lateral movement within the network.
Outdated Server Patches	**Server Maintenance Policy** • Schedule regular updates and patching of servers. • Maintain an inventory of server software versions and patch levels.	Unpatched servers are at risk of being exploited by known vulnerabilities, which could lead to severe data breaches.
Lack of Encryption	**Email Security Policy** • Mandate the use of email encryption for sensitive communications. • Implement secure email gateways to enforce encryption protocols.	Sending sensitive information over unencrypted channels exposes it to interception and unauthorized access.

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.

Least Privilege Access Control Policy

Policy Number: ACME-SEC-001

Version Number: 1.0

Effective Date: [Insert Date]

Purpose:
The purpose of this policy is to ensure that access to ACME Healthcare's systems and data is granted based on the principle of least privilege. This policy aims to minimize the risk of unauthorized access or misuse of privileges by employees, contractors, and third-party vendors.

Scope:
This policy applies to all employees, contractors, vendors, and any other individuals with access to ACME Healthcare's information systems and data.

Policy Statement:

1. **Access Authorization:**
    - Access to information systems, networks, and data will be restricted to those who require it to perform their job responsibilities.
    - All access requests must be approved by the relevant department head and IT Security.
2. **Role-Based Access Control (RBAC):**
    - Access will be granted based on job roles and responsibilities.
    - Roles will be clearly defined, documented, and reviewed annually.
3. **User Access Reviews:**
    - Quarterly access reviews will be conducted to ensure that users have appropriate access levels.
    - Any discrepancies or unauthorized privileges will be corrected immediately.
4. **Privilege Escalation Management:**
    - Privilege escalation must be formally requested, justified, and approved by IT Security and the employee's department head.
    - Temporary access will be time-bound and automatically revoked upon task completion.

5. **Access Revocation:**
    - Access will be immediately revoked for users who no longer require it due to role changes, termination, or other reasons.
    - Regular audits will be conducted to ensure compliance.
6. **Monitoring and Auditing:**
    - All privileged access will be logged and monitored.
    - Logs will be reviewed periodically to detect and respond to unauthorized access attempts.

Enforcement:
Violations of this policy may result in disciplinary actions, including termination of employment or contract and potential legal action.

Definitions:

- **Least Privilege:** The practice of limiting access rights for users to the bare minimum permissions they need to perform their work.
- **Role-Based Access Control (RBAC):** A method of regulating access to resources based on the roles of individual users within an enterprise.

Responsibilities:

- **IT Security:** Responsible for implementing and enforcing this policy, conducting access reviews, and responding to unauthorized access incidents.
- **Department Heads:** Ensure that access requests are justified and comply with the least privilege principle.
- **Employees and Contractors:** Ensure their access is used appropriately and report any access issues or unauthorized access.

References:

- NIST SP 800-53: Access Control (AC) Family
- ISO/IEC 27001:2013 – Information Security Management Systems

Approval:
Approved by: [Name, Title]
Date: [Insert Date]

Review Cycle:
This policy will be reviewed and updated annually or as required due to changes in technology or business processes.

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.

Instructions for Configuring and Managing Least Privilege Access

Step 1: Access Request Process

1. **Submit an Access Request Form:**
    - Complete the access request form available on the company's intranet.
    - Specify the system, data, or resource access needed, and justify why it's required for your job function.
2. **Approval Workflow:**
    - The request will be reviewed by the employee's manager and the IT Security team.
    - Approval or denial will be communicated via email within 2 business days.

Step 2: Role-Based Access Control (RBAC) Configuration

1. **Define Roles:**
    - Work with your department head to identify the specific roles and the access needed for each.
    - Document roles in the RBAC matrix template provided by IT.
2. **Assign Users to Roles:**
    - IT Security will assign users to the appropriate roles in the system.
    - Users will only have access to the resources defined in their role.

Step 3: User Access Review

1. **Quarterly Access Review:**
    - Department heads will receive a list of current access levels for their team members.
    - Review and confirm whether access is still required for each user.
    - Submit any changes or revocations to IT Security through the access management portal.
2. **Audit Reports:**
    - IT Security will generate audit reports to ensure compliance with the least privilege principle.

Step 4: Privilege Escalation Request

1. **Temporary Access Request:**
    - For temporary elevated access, submit a Privilege Escalation Request Form.
    - Include the task details, duration of access needed, and managerial approval.

2. **IT Security Review:**
    - The IT Security team will evaluate the request, configure temporary access, and set an automatic expiration.
3. **Completion and Revocation:**
    - Upon task completion, access will be automatically revoked.
    - Users must confirm task completion and notify IT Security if any issues arise.

Step 5: Access Revocation

1. **Employee Offboarding:**
    - HR will notify IT Security of any employee departures.
    - IT Security will disable the user's account and remove all access within 24 hours of notification.
2. **Periodic Cleanup:**
    - Conduct periodic checks to ensure no inactive accounts exist.
    - Deactivate accounts with no activity for more than 90 days unless otherwise justified.

Step 6: Monitoring and Logging

1. **Enable Logging:**
    - IT Security will configure systems to log all access to sensitive data and resources.
    - Logs will include user ID, timestamp, resource accessed, and action taken.
2. **Log Review:**
    - Set up automated alerts for suspicious activities.
    - IT Security will review logs bi-weekly and report any anomalies.

Step 7: Training and Awareness

1. **Mandatory Security Training:**
    - All employees must complete a security awareness training session on the least privilege principle and proper access management.
    - Training will be provided annually and upon any major updates to the policy.
2. **Ongoing Communication:**
    - Regular reminders and updates will be sent via email and posted on the company's intranet.

Step 8: Reporting Incidents

1. **Incident Reporting:**
    - If unauthorized access or misuse is suspected, report immediately to IT Security through the incident report form.
    - Provide details including user ID, time, and description of the incident.
2. **Incident Response:**
    - IT Security will investigate and take necessary actions, which may include revoking access, conducting audits, or involving law enforcement if required.

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.

Information Security Policy Implementation & Dissemination Plan: ACME Healthcare

1. Objectives

- Ensure all employees understand and comply with ACME Healthcare's information security policies.
- Minimize the risk of data breaches and security incidents.
- Foster a culture of security awareness within the organization.

2. Target Audience

- All employees (full-time, part-time, contractors)
- Third-party vendors with access to ACME Healthcare systems and data

3. Key Information

- **Policy Inventory:**
    - List of all relevant information security policies (e.g., Acceptable Use, Data Classification, Password Policy, Remote Access, BYOD, etc.)
- **Target Audience for Each Policy:**
    - Identify specific employee groups or roles that each policy applies to.
- **Communication Channels:**
    - Determine the most effective communication channels for each target audience:
        - Intranet
        - Email
        - Employee meetings/town halls
        - Departmental meetings
        - Posters/flyers
        - Security awareness training sessions (online or in-person)
        - Desktop notifications

- **Training Methods:**
    - Interactive training modules
    - Quizzes and assessments
    - Role-playing exercises
    - Case studies
    - Videos and presentations
- **Documentation:**
    - Policy acknowledgment forms
    - Training completion records
    - Communication logs

4. Implementation Timeline

- **Phase 1: Policy Review & Updates**
    - **Task:** Review and update all existing policies to ensure they are current, comprehensive, and easy to understand.
    - **Timeline:** 1-2 months
    - **Departments Involved:** IT, Legal, Human Resources
- **Phase 2: Communication & Awareness**
    - **Task:** Develop and implement a communication plan to disseminate policies to all employees.
    - **Timeline:** Ongoing
    - **Events:**
        - Policy launch event (e.g., company-wide email, intranet announcement)
        - Regular security awareness campaigns (e.g., phishing simulations, security tips)
        - Quarterly security newsletters
    - **Departments Involved:** IT, Communications, Human Resources, Legal
- **Phase 3: Training & Education**
    - **Task:** Conduct mandatory security awareness training for all employees.
    - **Timeline:** Ongoing (e.g., annual refresher training)
    - **Events:**
        - Online training modules
        - In-person workshops
        - Departmental training sessions
    - **Departments Involved:** IT, Training & Development, Human Resources
- **Phase 4: Policy Acknowledgement & Compliance**
    - **Task:** Obtain employee acknowledgment of policy receipt and understanding.
    - **Timeline:** Ongoing
    - **Methods:**
        - Online acknowledgment forms
        - Employee signatures
    - **Departments Involved:** IT, Human Resources

5. Monitoring & Evaluation

- **Track key metrics:**

    - Training completion rates
    - Number of policy violations
    - Effectiveness of communication channels
    - Employee feedback on training and awareness campaigns
- **Conduct periodic reviews:**
    - Assess the effectiveness of the implementation plan.
    - Identify areas for improvement and make necessary adjustments.

6. Roles & Responsibilities

- **IT Department:**
    - Lead the implementation and ongoing management of the plan.
    - Develop and maintain security policies.
    - Conduct security assessments and audits.
    - Provide technical support and guidance.
- **Human Resources Department:**
    - Coordinate employee training and awareness programs.
    - Ensure compliance with employment laws and regulations.
    - Assist in the investigation and resolution of security incidents.
- **Communications Department:**
    - Develop and disseminate communication materials related to security policies.
    - Manage internal and external communication channels.
- **Legal Department:**
    - Provide legal and regulatory guidance on security matters.
    - Review and approve all security policies.

7. Budget & Resources

- Allocate budget for:
    - Training materials and tools
    - Security awareness campaign materials
    - Communication platforms
    - External training resources (if applicable)

Reflexions

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.