Risk Management Report

Project Title: Develop and Apply Risk Management Strategies

1. Introduction

This report demonstrates the practical application of risk management strategies based on the results of a vulnerability scan. The aim is to identify and assess cybersecurity risks, provide treatment recommendations, implement basic mitigation steps, and establish a procedure for ongoing risk monitoring.

2. Vulnerability Scan Summary

A network vulnerability scan was conducted using an industry-standard scanning tool. The scan identified several security weaknesses, with two classified as critical due to their high impact and likelihood of exploitation.

3. Critical Risk Assessments

3.1 Critical Risk #1: Apache HTTP Server Path Traversal (CVE-2021-41773)

- **Description**: This vulnerability allows path traversal in Apache HTTP Server versions 2.4.49 and 2.4.50. An attacker can gain access to files outside the document root, and potentially execute remote code.
- **Impact**: High – Unauthorized access and remote code execution.
- **Likelihood**: High – Public exploits exist and are actively used.

Treatment Recommendation

- **Action**: Immediately patch Apache HTTP Server to version 2.4.51 or higher.
- **Justification**: This vulnerability is known and widely exploited. Patching eliminates the attack vector.

Basic Mitigation Steps

1. Identify all servers running vulnerable versions.
2. Apply latest updates from Apache.
3. Disable unnecessary modules and services.

4. Test server functionality post-patch to ensure stability.

3.2 Critical Risk #2: Default Credentials on Network Router (admin/admin)

- **Description**: The default administrative credentials on a router are unchanged, allowing unauthorized access to network settings.
- **Impact**: Critical – Potential for complete network compromise.
- **Likelihood**: High – Easily exploited with minimal skill.

Treatment Recommendation

- **Action**: Change default credentials to a unique, strong password.
- **Justification**: Default credentials are a top attack vector. Changing them closes this obvious gap.

Basic Mitigation Steps

1. Change admin username and password immediately.
2. Disable remote access to the router interface.
3. Update router firmware to the latest version.
4. Implement multi-factor authentication if supported.

4. Additional Risk Identifications (Non-Critical)

Risk ID	Description	Severity	Recommendation
R3	TLS 1.0 protocol enabled	Medium	Disable TLS 1.0; enforce TLS 1.2+
R4	Missing secure cookie flags	Low	Set HTTPOnly and Secure cookie flags
R5	Open Telnet port detected	Medium	Disable Telnet; enable SSH

5. Risk Monitoring Procedure

Procedure Title: Ongoing Risk Monitoring Framework

Objective

To continuously track and manage cybersecurity risks identified during initial and future scans.

Procedure Steps

1. **Weekly Vulnerability Scans**:
    - Use tools like Nessus/OpenVAS to conduct scheduled scans.
    - Focus on recurring vulnerabilities and configuration issues.
2. **Update Risk Register**:
    - Maintain a live document of all risks.
    - Include fields: risk ID, status (Open/Mitigated), owner, last review date.
3. **Alert Configuration**:
    - Enable notifications for critical issues or recurrence.
    - Integrate with SIEM for real-time monitoring.
4. **Monthly Review Meetings**:
    - Cross-functional teams meet to review open issues.
    - Assess treatment effectiveness and update strategies.
5. **Audit Logs and Change Tracking**:
    - Monitor system logs for unauthorized changes.
    - Investigate anomalies and document findings.

Justification

Ongoing monitoring ensures prompt detection of re-emerging threats and validates the effectiveness of existing controls.

6. Conclusion

Risk management is an ongoing process. Identifying critical risks, applying timely treatments, and maintaining effective monitoring procedures are key to reducing an organization's security exposure. The strategies presented here align with industry best practices and provide a proactive framework for organizational cybersecurity.