Activity - Vulnerability Assessment Report

1st January 20XX

Activity Overview

This project focuses on performing a comprehensive vulnerability assessment for an organization's IT infrastructure. The goal is to identify potential weaknesses, evaluate the level of risk they pose, and provide actionable recommendations to mitigate or eliminate these vulnerabilities. This report highlights my ability to systematically assess an organization's security posture and provide insights to enhance its defense mechanisms.

Scenario

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server since many of the employees work remotely from locations all around the world. Employees of the company regularly query or request data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

A vulnerability assessment can help you communicate the potential risks to the company's decision-makers. You must create a written report that clearly explains how the vulnerable server risks business operations and how it can be secured.

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server serves as a centralized computer system responsible for storing and managing substantial volumes of data. Specifically, it houses customer information, campaign data, and analytics. These stored data points are later analyzed to track performance and tailor marketing efforts. Given its frequent use in marketing operations, ensuring the security of this system is critical.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9
Employee	Disrupt mission-critical operations	2	3	6
Customer	Alter/Delete critical information	1	3	3

Approach

We assessed risks by examining the business's data storage and management procedures. We evaluated the likelihood of threat occurrences and their potential impact, considering the risks to day-to-day operational requirements.

Remediation Strategy

To enhance database security, we recommend implementing the following measures:

1. **Authentication, Authorization, and Auditing:**
    - Ensure that only authorized users can access the database server.
    - Utilize strong passwords, role-based access controls, and multi-factor authentication to limit user privileges.
2. **Data Encryption in Motion:**
    - Use Transport Layer Security (TLS) instead of Secure Sockets Layer (SSL) to encrypt data while it's in transit.
    - TLS provides stronger security and better protection against vulnerabilities.
3. **IP Allow-Listing:**
    - Restrict database access by allowing only specific IP addresses (such as corporate offices) to connect.
    - This prevents random internet users from accessing the database.

Conclusion

The vulnerability assessment revealed several critical and high-severity vulnerabilities that could compromise the organization's security if left unaddressed. By implementing the recommended actions, the organization can significantly reduce its risk exposure and improve its overall security posture. This project highlights the importance of proactive vulnerability management and demonstrates my ability to identify, analyze, and prioritize vulnerabilities effectively.