Vulnerability Assessment Report

Vulnerability Assessment Project – E-Commerce Database Server

Overview

As part of my cybersecurity training, I conducted a vulnerability assessment for a simulated e-commerce company. The project focused on evaluating risks associated with a publicly accessible database server and recommending remediation strategies to improve security. This exercise allowed me to practice applying NIST SP 800-30 guidelines and develop the skills required to communicate technical risks to business decision-makers.

System Description

- **Infrastructure:** Linux server with MySQL database
- **Resources:** High-performance CPU, 128GB RAM
- **Connections:** IPv4 networking, SSL/TLS encryption enabled
- **Use case:** Stores customer, campaign, and analytics data for global remote teams

Scope

The assessment was limited to **access controls** and the risks posed by leaving the database server open to the public. The review period was set to three months, and NIST SP 800-30 Rev. 1 guided the analysis.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.

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*

Key Finding: The highest risk came from external hackers exploiting the open public access to the database.

Approach

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

Remediation Strategy

To mitigate risks, I recommended:

- Enforcing **authentication, authorization, and auditing (AAA)** controls
- Using **role-based access control (RBAC)** and **multi-factor authentication**
- Migrating from **SSL to TLS** for secure communication
- Implementing **IP allow-listing** to restrict access only to corporate networks

Key Skills Demonstrated

- Vulnerability assessment using structured methodology (NIST SP 800-30)
- Risk analysis and scoring (likelihood × severity)
- Development of remediation strategies (technical and procedural)
- Clear technical documentation for non-technical decision makers