Vulnerability Assessment Report

11th March 2025

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.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to 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 Linux** operating system and hosts a **MySQ**L database management system. It is configured with a stable network connection using **IPv4 addresse**s and interacts with other servers on the network. Security measures include **SSL/TLS** encrypted connections.

- General notes:
    - Server needs to be accessible by only the remote employees such that access is not given to outsiders.
    - Currently the database is open to the public, this is a crucial issue that I as an Analyst must solve.
    - Server interacts with other servers on the network & data is encrypted using SSL/TLS.

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 March 2025 to June 2025 NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The Database Server is a centralized database running MySQL which efficiently manages customer data which could also be vulnerable to SQL injection and MITM attacks, making data protection critical. Its high-spec design exceeds demands for handling queries, enabling fast retrieval of purchase histories and buying habits to attract potential customers. Without these capabilities, regular marketing operations would cease to exist.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	Conduct "man-in-the-middle" attacks	*3*	*3*	*9*
Employee	*Insider misuse / data theft.*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

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

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.