Identifying vulnerabilities for a small business

**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.

Vulnerability Assessment Report:

# 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 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](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

*The database server contains a collection of organised data and information which are valuable to the business. They also perform complex tasks while assessing data. It is important for the business to secure the data on the server because there is a massive amount of data stored in the database and it is accessed by multiple users simultaneously. An organisation runs their operations daily using the database, and disrupting or disabling it will affect the running of businesses.*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Can infiltrate into the organisations system leading to data breach or data manipulation* | *3* | *3* | *9* |
| *Employees* | *Can knowingly or unknowingly commit lead to exposing of data or damaging business equipments* | *1* | *2* | *2* |
| *Competitor* | *Purposely stealing, exposing, deleting, or editing the data their gain* | *1* | *3* | *3* |

# Approach

I chose hackers, employees and competitors as the threat sources through the risk assessment. Hackers can be a very critical threat due to their ability to exploit vulnerabilities for data breaches or data manipulation which can ruin the reputation of the organisation. Employees can deliberately or unintentionally have the ability to expose sensitive data or damage the business equipment. Competitors may target the organisation by stealing, deleting or editing the valuable information. All these can affect the reputation, financial stability, competing position and the market value.

# 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.