**Vulnerability Assessment Report**

**1st January 2023**

## Scenario



Review the following scenario. Then complete the step-by-step instructions.

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 of the situation can help you communicate the potential risks with decision makers at the company. You must create a written report that clearly 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 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 is valuable because employees of the company regularly query, or request, data from the server to find potential customers. It is important to secure the data on the server because its contains valuable information about potential customers that is used by the employees of the business and if the data on the server in compromised it could result in major losses for the business. If the server is compromised employees won’t be able to access the data of the potential clients and thus employees won’t be able to conduct their duties which would result in a loss of profits. 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** |
| *Competitor* | *Obtain sensitive information via exfiltration or Dos the Server.* | *1* | *3* | *3* |
| *Hacker* | *Place ransomware on the database preventing access till demands are met or DoS the server.* | *3* | *3* | *9* |
| *Employee* | *Disgruntled employees could sell and damage data containing potential customers* | *2* | *3* | *6* |
| *Malicious Software* | *Malicious Software could be uploaded to the database* | *1* | *2* | *2* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

# Approach

In a tough market, rivals are constantly seeking an edge. While some may resort to corporate espionage, the risk is high as they could face legal consequences if caught. Hackers might install ransomware on the server, blocking access until their demands are met. This is typically done to extort money. Unhappy employees might sell or sabotage data containing potential customer information. Malicious software could be uploaded to the database to disrupt the company and extract value from the situation. Risks that were measured consider 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 was weighed against the impact on day-to-day operational needs.

# Remediation Strategy

Implementation of authentication, authorization, Accounting, 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. Implementing Multi-factor authentication (MFA) to prevent unauthorized access if the Threat actor manages to gain the login credentials. Keeping track of who accesses the database, when they access the database, and where they access the database. This will allow us to tell who could be negatively impacting the database after hours. Implementing the principle of least privilege to prevent employees from having more access than they need to perform their tasks.