**Portfolio activity on :**

**Vulnerability Assessment Report**

**1st January 2024**

# 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 2024to August 2024. [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 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.

* The database server is a valuable asset to the business because it stores information such as data, on a remote database server, since many of the employees work remotely from locations all around the world and use it to query and request data from a server to find potential customers.
* Keeping the database server open to the public is a serious vulnerability .It is important for the business to secure the data on the server because the database contains sensitive information that should not be easily available to everyone. Not securing the database makes the server vulnerable and more likely to be at risk from threat actors as it is easy to access due to weak or lack of security.
* If the data server is disabled it could have major security risks. As a threat actor could examine and assess the company's vulnerabilities over time using various tools or could alter or delete data that is critical to day-to-day business operations.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Employee | Craft counterfeit certificates.  Could compromises a certificate  authority to make their connections appear legitimate. | 2 | 1 | 2 |
| Competitor | Obtain sensitive information via exfiltration.Could installs malicious software on organizational systems to locate and acquire  sensitive information that could be potentially used against the organization. | 1 | 3 | 3 |
| Hacker | Conduct "man-in-the-middle" attacks.Threat actor could eavesdrop on sessions between  internal and external systems. Later, they relay messages between organizational and external systems that make them believe they're talking directly to each other over a private connection. | 3 | 3 | 9  (Likelihood x Severity=  Risk) |

# 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.

The likelihood of an employee crafting a counterfeit certificate is level 2 because if an employee gets the opportunity they may be tempted to take advantage of the unsecure database. The impact of this potential event would not really affect the business operations of the organization.

The likelihood of a Competitor obtaining sensitive information via exfiltration is a Level 1 as it is not likely to happen ,but if it were to happen the severity of such an event would be a level 3 as it could potentially stop and largely disrupt business continuity.

The likelihood of a Hacker conducting a “man-in-the-middle” attack is a level 3 because a hacker would want to gain as much information before their official attack and the severity of this event is a level 3 because it could stop/disrupt business continuity .

# 

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server which will prevent events such as crafting counterfeit certificates . This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. To prevent the event of the “man-in-the-middle”attack you need to encrypt data in motion using TLS instead of SSL. To prevent random users(competitors) from obtaining sensitive information use IP allow-listing to corporate offices to prevent them from the internet from connecting to the database.