

# Vulnerability Assessment Report

19<sup>th</sup> August 2023

---

## 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 March 2023 to May 2023. [NIST SP 800-30 Rev. 1](#) is used to guide the risk analysis of the information system.

## Purpose

The company database is the centralized computer system which is storing and managing large amounts of sensitive data. The server is used to store customer, campaign and analytic data that can be used later to analyze performance and personalize the marketing efforts. It is critical to secure the system because it is regularly used by the company employees

## Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
<i>Hacker</i>	<i>Obtain sensitive information via exfiltration</i>	3	4	9
<i>Employee</i>	<i>Disrupt critical operations</i>	2	4	5
<i>Customer</i>	<i>Alter/Delete critical information</i>	1	3	3

## **Approach**

Risks that were measured considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to 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.