Vulnerability Assessment Report

May 2025

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 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The system is a database server which is used for storing information related to the customer, campaign and analytic data that would be important in the future use for business. It is important to secure these data on the server because of its regular uses for marketing operation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Networking	*Failed connection to other servers in the network*	*1*	*2*	*2*

Hacker	*Obtain information through exfiltration*	*3*	*3*	*9*
Employer	*Might leak some information*	*2*	*2*	*6*
Customer	*Might delete or alter 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.