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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

A database is very important to the business because it serves as the backbone of the business operations of the company. It 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 be later analyzed to track performance and personalize marketing efforts. Additionally, ymployees of the company regularly query, or request, data from the server to find potential customers. It is important for the business to secure its data on the server to avoid any alterations to that database and protect information from being stolen by threat actors. If the server was disabled it would cause catastrophic effects to business operations and assets.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Disrupt mission-critical operations.*	*3*	*3*	*9*

Employee	*Alter/Delete critical information*	*1*	*2*	*2*

Approach

Since the company's database server is open to the public, the threat sources are likely to be human and unlikely to be technical in nature due to the functionality and resources of the server. Therefore the likely threat sources are either hacker, competitor, or an employee. An employee is a threat source because they can unintentionally alter/delete critical information which could significantly reduce the functionality of the company's business ops and assets. A hacker also is a threat source and can intentionally disrupt mission-critical ops of the org which has a high likelihood to occur due to easily accessing the database server.

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.