Vulnerability Assessment Report

23rd March 2025

Benjamin Taylor – Google Cybersecurity

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 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this security analysis is to ensure the continued integrity, confidentiality, and availability of the database server, which is a critical component of the business's operations. This server stores sensitive information for both the business and customers, making it important to protect against unauthorized access and potential data breaches. If the server were to be compromised, the business could significantly suffer through operational disruptions, financial loss, and even damage to their reputation. By assessing and addressing vulnerabilities, the organization aims to strengthen its security posture and support the continuity of business.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*Alter or Delete Critical Information*	*1*	*3*	*3*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*

Approach

Risks 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.