Vulnerability Assessment Report

September 23

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 July 2023 to September 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system. The scope for this analysis is specific to the integrity of the data held within the server hardware.

Purpose

Many employees access this specific server from across multiple remote locations. The data held within the server hardware is the primary source of information used to direct organization workflow. It is important to secure this data as it is the primary element of our organization that facilitates multiple sections of our employees to conduct their work. If the web server becomes disabled or the data loses integrity our organization would no longer be able to function until the web server is brought back online, and its data verified.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information from public facing database*	*2*	*2*	*4*
Outsider	*SSL vulnerabilities become targeted by threat actor*	*1*	*3*	*3*
Natural Hazards	*Natural disaster destroys the organizations server hardware*	*1*	*3*	*3*

Approach

The business assessed the data storage and management approaches, taking into account the probability of potential threats occurring and the consequences they might have on daily operational requirements.

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. Backup server data on location or hold backups off sight of server hardware, develop a disaster plan to allow for swift migration of backup assets to a deployable server at scale.