Vulnerability Assessment Report

28th July 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 June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The company uses a remote database server that its employees use on a regular basis. The employees of said company work remotely from locations all around the world. Meaning that these employees need access to this information on the database daily to do their jobs. If they lose access, then that would result in lost business…lost revenue. Also, the company has had the server open to the public for the past three years…since it has been open. Meaning, The PII of the clients we service isn't protected from malicious actors that could sell this information or further compromise the company if threat persists. Therefore, we will conduct an assessment it to identify any vulnerabilities and provide remediation strategies for those vulnerabilities if we can.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Employee	*Alter/Delete critical information*	*1*	*3*	*3*
Competitor	*Conduct Denial of Service (DoS) Attacks*	*2*	*3*	*6*
Power Outages	*Disrupt mission-critical operations*	*1*	*3*	*3*

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.

I selected the three threat sources and events that I outlined above to illustrate the different way the company's server can be impacted. First, employees can unwillingly alter or delete data while access the server. Second, competitors could conduct Denial of Service (DoS) attacks that could slow down or disrupt business operations entirely. Finally, if a power outage where to occur, then the company would lose its ability to conduct normal business. All these threat sources and events need to be considered when developing remediation strategies.

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. A firewall can be implemented to provide port filtering or IP blocking when there is a suspected Denial of Service (DoS) attack. The company will also need to implement the principle of least privilege to only give access to those employees who need access. Finally, the company needs to investigate backup systems for key infostructure. For instance, if the power goes out, the company should have a backup generator to ensure system access is maintained.