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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is critical to the business as it stores and manages all business-critical data. Securing the data on the server is paramount to protecting sensitive business information, customer data, and operational records. If the server were disabled, it could disrupt business operations, lead to data loss, and compromise the integrity and confidentiality of business information.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Outsider (Hacker)	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
System admin	*Deletes or alters information on accident*	*1*	*3*	*3*
Natrual hazard	*Could stop everything from working*	*1*	*2*	*2*

Approach

I looked at how our data is stored and managed to figure out the biggest risks. I thought about how likely different threats are and how bad they could be if they happened. This helped me see which threats are the most serious so I can focus on those. I picked threats like hackers trying to steal data, system admins accidentally messing up information, and natural hazards that could disrupt everything. By tackling these risks, I want to keep our database server running smoothly and securely.

Remediation Strategy

To deal with these risks, I'm going to set up strong authentication and authorization methods. This means using strong passwords, role-based access controls, and multi-factor authentication to make sure only the right people can access the database server. I'll also encrypt data using TLS instead of SSL to make it more secure. Plus, I'll use IP allow-listing to restrict access to just our corporate offices, keeping random internet users out. By doing all this, I aim to protect our database server and keep our data safe.