Vulnerability Assessment Report

1st January 20XX

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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

After reviewing the organization, I feel that it is imperative that the organization makes some immediate changes to the way that their servers are handled. If customer information was handled incorrectly, the financial and reputational losses could be very substantial. Hence, a threat assessment could help point out any weakness, and bolster the organizations' security posture.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Malicious Software	*Conduct Denial of Service (DoS) attacks.*	*2*	*3*	*3*
Natural Hazards	*Power outage; extreme weather events.*	*1*	*3*	*3*

Hacker	*Can alter or delete customer information*	*2*	*2*	*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. **After conducting my threat assessment, I chose three threat sources that I deemed most detrimental to the organization. They were malicious software, hackers, and natural hazards. Firstly, If someone were to commit a DDos Attack on the server, it could halt business operations, and stop productivity. Secondly, if a hacker were to alter or delete sensitive customer information, it could cost the company huge sums for not complying with regulations and loss to reputation. Lastly, because the server is held at one physical location, it is at great risk to natural hazards. Though the odds of inclement weather may not be high, if it were to take place, all company information could be lost.**

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. **After running the threat assessment, I believe that the database should be placed with a cloud service provider. It would be more beneficial with scaling, and the customer's info would be better protected from natural hazards, to name a few. Also, the company should practice lease of privileges, and no longer allow the database server free to the public. They should also enable MFA sign-ons, and monitor who does have access to the servers.**