Vulnerability Assessment Report

1st January 20XX

Kevin Landry

Cybersecurity Analyst

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?- Correlating the value of a system with the risk it presents is critical in understanding the potential impact of an incident on systems such as a company's server. Depending on how much a business depends on the system dictates the amount of time and resources spent ensuring it's secure.*
- *Why is it important for the business to secure the data on the server? The server contains PII of customer's data which is extremely sensitive and a frequent target of bad actors in the cyber space, If an attacker is able to infiltrate the system via SQL injection, for example, the company runs the risk of everything contained on the server being stolen and sold or ransomed.*
- *How might the server impact the business if it were disabled? The business would come to a screeching halt. Customer's trust in the company would be negatively impacted leading to loss of revenue and catastrophic damage done.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker-Insider Threat	*Threat source installs or executes malicious software to exfiltrate sensitive data.*	*3*	*3*	*9*
Operating System(s) Vulnerability	*Exploitation of zero-day vulnerability in MySQL server allowing unauthorized data access*	*1*	*3*	*3*

Approach

In evaluating the risks to the company's public-facing database, I focused on common threat sources and events that could exploit the server's current vulnerabilities. These include external cybercriminals aiming to exfiltrate sensitive customer information, malicious insiders who may misuse legitimate access, and potential zero-day vulnerabilities in the MySQL server that could be exploited remotely.

This qualitative assessment used a severity-likelihood framework, considering the probability and potential impact of each threat source on the company's daily operations and reputation. Prioritizing high-severity threats helps ensure that the most critical risks are addressed first, especially those that could compromise customer trust and disrupt business continuity. By identifying these specific risks and proposing targeted mitigations, this assessment aims to minimize exposure and strengthen the security of customer data.

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.