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

The database server is valuable to the business as it stores crucial information for customer queries and potential sales opportunities. The business needs to secure the data on the server to protect sensitive customer information and maintain business continuity. If the server were disabled, it would significantly impact the business's ability to serve customers and conduct operations effectively.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee (Privileged User)	*Unauthorized access to sensitive data*	*2*	*3*	*6*
Hacker (Outsider)	*Attempted unauthorized access to the database server*	*3*	*3*	*9*
Malicious Software (Malware)	*Ransomware attack on the database server*	*2*	*3*	*6*

Approach

I assessed risks based on how the business stores and manages data. I identified potential threats and events by considering the likelihood of a security incident due to the open access permissions of the information system. We compared the severity of potential incidents with their impact on daily operations.

1. **Employee (Privileged User) Threat**: This is when someone inside the company accesses sensitive data without permission. It's risky because it can lead to leaks or breaches of important information.
2. **Hacker (Outsider) Threat**: This is when someone from outside the company tries to get into the system without permission. It's dangerous because it can expose confidential data to unauthorized people.
3. **Malicious Software (Malware) Threat**: This is a type of attack where harmful software can disrupt operations or damage data. It's a serious threat because it can cause major problems for the company's systems.

Remediation Strategy

To fix these risks, we can use some simple security measures:

1. Principle of Least Privilege: Give employees and users only the access they need to do their jobs. This reduces the chance of someone accessing data they shouldn't.
2. Defense-in-Depth: Add layers of security like firewalls and antivirus software to protect against different types of attacks. This makes it harder for hackers to get in.
3. Multi-Factor Authentication (MFA): Use more than one method to verify a user's identity, like a password and a code sent to their phone. This adds an extra layer of security.
4. Authentication, Authorization, and Accounting (AAA) Framework: Use tools that keep track of who is accessing what data and when. This helps detect any unusual activity and stops unauthorized access.
5. 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.