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 business database is an integral part of the overall function of what the business needs to do. This database contains a large amount of private data that may or may not be critical to the functions of the company along with PII(Personal Identifying Information) of employees and customers. Due to the potential risk of a breach, it is greatly recommended for the database to be as secure within practical limits. A breach of this critical system will often lead to an adverse effect on reputation, confidentiality, integrity, and availability of the data within the database.

According to gathered information, it's shown that the company's database has been open to the public for the past 3 years, this is a critical problem and needs to be remediated as soon as possible. The purpose of this report is to display the potential sources that may act upon an unsecured database, the type of event they may cause, and the overall impact and likelihood of said event happening.

Risk Assessment

Threat source	Threat events	Likelihood	Severity	Risk
Employee with admin privileges	-Disrupt mission-critical operations -Alter/Delete critical information	*2*	*2*	*4*
Employee or Customer	-Alter/Delete critical information -Disrupt mission-critical operations	*1*	*2*	*2*
Hacker *APT*	-Obtain sensitive information via exfiltration -Alter/Delete critical information	*3*	*3*	*9*

Approach

Likelihood, severity, and risk was measured based on the potential of an attack from the threat source as well as the severity that I may be caused by the event the entity may enact. Likelihood was determined based on the potential for an event to be carried out on the vulnerable system. Severity was determined based on the overall effect that the event would have on everyday business operations. Risk was determined based on the relation between the likelihood of an event happening and the severity of the event(Likelihood X Severity = Risk).

Remediation Strategy

To correct and mitigate the potential vulnerabilities that the open database will cause, the company must use these security controls to mitigate/remediate the risk identified above. These security measures are:

1. Principle of least privilege
    a. To ensure that only those who need access to the data are the only ones to access it, rejecting anyone who has no legitimate need to access said information to perform their duties.
2. Defense in depth
    a. To ensure that no malicious threat actors are able to access the data without getting through a diverse security setup. This is preventative and mitigates the

risk however this does not guarantee that no threat actors are able to breach the system.

3. Multi-factor Authentication(MFA)
    a. To ensure that employee and admin(privileged) accounts aren't susceptible to brute force attacks, greatly reducing the likelihood of a privileged account being accessed illegitimately
4. Authentication, Authorization, Accounting(AAA) framework
    a. To ensure that a user is who they say they are(Something they have, know, or are), ensure that they have access to said item(Least Privilege), and to ensure that all movements and access to said items are accounted for and recorded(logs)