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?*
  A database server is invaluable to a business as it serves as a central repository for data, ensuring consistency, security, and efficient management. It enhances performance by handling complex queries and transactions, while its scalability allows it to grow with the business. Robust security measures protect sensitive information, and automated backup and recovery solutions ensure data integrity and reliability. Additionally, a database server supports business intelligence and analytics, enabling informed decision-making through comprehensive data analysis and reporting.
- *Why is it important for the business to secure the data on the server?*
  Securing the data on a server is crucial for a business because it protects sensitive information from unauthorized access, breaches, and cyberattacks, which can lead to financial losses, legal consequences, and damage to the company's reputation. Ensuring data security also helps maintain customer trust and compliance with regulatory requirements, safeguarding personal and financial data. Moreover, secure data management ensures business continuity by preventing data loss or corruption, allowing for reliable and efficient operations.
- *How might the server impact the business if it were disabled?*
  If a server were disabled, the business would face significant disruptions, including operational downtime that halts productivity and delays critical tasks. Employees would be unable to access essential data, impairing decision-making and daily operations.

Customer-facing services, such as websites and support systems, would become unavailable, leading to dissatisfaction and potential loss of business. Financial losses would mount due to immediate revenue drops and longer-term impacts from decreased customer trust. Additionally, the risk of data corruption or loss could complicate recovery efforts, while prolonged outages and security breaches would damage the company's reputation. Compliance issues may also arise, potentially resulting in fines and legal consequences.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Malicious Software	*Infecting any system, may lead to infecting all the systems in the network and may lead to system malfunctions, shutdowns and/or data leaks*	*2*	*3*	*6*
Faulty power supplies	*Equipment failures caused by operational environments*	*2*	*2*	*4*

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.

Since the device is connected to other servers on the network, a malicious software installed accidentally can lead to failures of multiple servers and also data leaks which may prove to be very detrimental to the company. Faulty power supplies may also risk saving the data into the database correctly, or even cause interruptions while working with data, which may impact the work and may affect the data in the database.

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.

Also keeping track of any new software getting installed into the systems or connecting peripheral devices such as usb or flash drives to the computer needs to be kept track of and assessed. Regularly checking hardware components and power supplies is important to prevent sudden, unexpected malfunction.

Some of the other preventive measures could be to set up the following, if not implemented already

- Principle of least privilege
- Defense in depth
- Multi-factor authentication (MFA)
- Authentication, Authorization, Accounting (AAA) framework