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 contains critical customer data used for identifying potential customers and conducting market analysis. Securing the data on this server is essential to protect the company's reputation, maintain customer trust, and ensure compliance with data protection regulations. If the server were to be compromised or disabled, it could lead to significant financial losses, operational disruptions, and legal liabilities.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External Attackers	*Unauthorized access*	*3*	*3*	*9*
Malicious Insiders	*Data Exfiltration*	*2*	*3*	*6*
Business Competitors	*Denial of service (DoS) Attack*	*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. External attackers pose a high risk due to the likelihood of exploiting the publicly accessible database to gain unauthorized access. Malicious insiders, though less frequent, can exfiltrate sensitive data, leading to severe confidentiality and integrity issues. Business competitors might initiate DoS attacks to disrupt services, impacting availability and customer satisfaction.

Remediation Strategy

Implement Multi-Factor Authentication (MFA): Require MFA for all access to the database server to ensure that only authorized users can gain entry, reducing the risk of unauthorized access by external attackers.

Principle of Least Privilege: Enforce strict access controls by granting employees only the minimum necessary permissions to perform their jobs. This reduces the risk of data exfiltration by malicious insiders.

Defense in Depth: Employ multiple layers of security measures, including firewalls, intrusion detection systems, and regular security audits, to protect against DoS attacks and other threats. This layered approach ensures that if one defense fails, additional measures are in place to protect the system.