Vulnerability Assessment Report

16 April 2025

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 April 2025 to July 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

This vulnerability analysis aims to assess the risks associated with the company's publicly accessible remote database server. The server holds valuable customer prospect information that employees rely on to generate business opportunities.

Keeping this data unprotected threatens the organization's reputation, operational continuity, and may expose it to financial penalties or data breaches. This assessment will provide actionable recommendations to secure the server and support the company's long-term growth and compliance efforts.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk** (Likelihood x Severity=risk)
Employee	*Alter/Delete critical information*	*1*	*2*	*2*
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Disrupt mission-critical operations*	*3*	*3*	*9*

Approach

This vulnerability assessment focused on identifying the most probable and impactful threats to the company's public-facing database server. The selected risks were chosen based on their relevance to the company's operations, the sensitivity of stored data, and the open nature of the system. Likelihood scores were determined by assessing how easily each threat actor (e.g., employees, competitors, hackers) could exploit the exposed database. Severity scores reflected the potential damage to business operations, data integrity, and reputation.

Remediation Strategy

To address the identified risks, a combination of technical and managerial controls should be implemented. To mitigate the risk of sensitive data exfiltration by competitors or hackers, the database should be moved behind a firewall, with strict access controls based on the principle of least privilege, and access should be restricted to VPN-authenticated users. Multifactor authentication (MFA) should be enforced to prevent unauthorized access. Additionally, auditing and logging mechanisms should be implemented to monitor employee access and detect any unauthorized changes. These controls will significantly reduce the likelihood and impact of data breaches, improving the overall security posture of the system.