Vulnerability Assessment Report

11th March 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 focuses on the security risks associated with the company's publicly accessible database server**.** The assessment will evaluate threats that impact the confidentiality, integrity, and availability (CIA**)** of the stored customer and business data. This evaluation excludes physical security concerns, external IT systems, and unrelated infrastructure components. The goal is to identify vulnerabilities in network security**,** access controls, and potential exploitation methods**,** ensuring that the database remains protected from cyber threats such as unauthorized access, SQL injection, and denial-of-service (DoS) attacks**.**

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

Purpose

- The database server is essential for storing and managing customer and business data, enabling employees to access potential customer information and support decision-making. It plays a critical role in the company's remote work environment, ensuring seamless operations.
- Securing the database is vital to protect sensitive information from unauthorized access, cyber threats, and data breaches. A security compromise could lead to financial losses, reputational damage, and legal penalties due to non-compliance with data protection regulations.
- If the database server is disabled due to a cyberattack or system failure, employees will be unable to access essential business data, disrupting daily operations. This could result in missed business opportunities, decreased productivity, and loss of customer trust

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hackers (External Threat)	*Conduct SQL Injection to extract sensitive customer data.*	*3*	*3*	*9*
Malicious Insider (Employee or Competitor)	*Exfiltrate business-critical data from the database*	*2*	*3*	*6*
Denial-of-Service (DoS) Attackers	*Overwhelm the database with excessive requests, causing downtime*	*3*	*2*	*6*

Approach

This qualitative vulnerability assessment focuses on three major threats that pose significant risks to the company's publicly accessible database server. SQL Injection was selected because it is a common attack that can lead to data breaches and unauthorized access to sensitive customer information. Malicious insiders represent an internal risk, where employees or competitors may exfiltrate business-critical data, leading to financial and reputational damage. Denial-of-Service (DoS) attacks were included because they can disrupt business operations, preventing remote employees from accessing essential data. These threats were chosen due to their high impact on data security, business continuity, and regulatory compliance.

Remediation Strategy

To mitigate SQL Injection attacks, the company should implement prepared statements and parameterized queries to prevent malicious input execution. A Web Application Firewall (WAF) can also help filter out SQL injection attempts. To reduce the risk of data exfiltration by malicious insiders, the company should enforce the Principle of Least Privilege (PoLP), ensuring employees only have access to necessary data. Additionally, Multi-Factor Authentication (MFA) and role-based access controls (RBAC) should be implemented to secure database access. To prevent Denial-of-Service (DoS) attacks, rate limiting, traffic filtering, and network redundancy should be deployed to maintain availability. Continuous monitoring and logging using the Authentication, Authorization, and Accounting (AAA) framework will help detect and respond to threats in real time.