Vulnerability Assessment Report

17th May 2025

Purpose

The database server is a critical asset that stores customer and prospect information used for sales operations. It supports business growth by enabling remote employees to access data from any location. Securing this data is vital to maintaining customer trust, regulatory compliance, and competitive advantage. If the server is disabled or compromised, the company could suffer data breaches, operational disruption, or reputational damage, which may lead to financial losses.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker (external)	Obtain sensitive information via exfiltration	3 (High)	3 (High)	9
Competitor	Conduct Denial of Service (DoS) attack	2 (Moderate)	3 (High)	6
Insider (employee or contractor)	Alter/delete critical information	2 (Moderate)	2 (Moderate)	4

Approach

This assessment used a qualitative approach guided by NIST SP 800-30 Rev. 1 to identify key risks related to the publicly accessible database server. The three threat sources—external hackers, competitors, and insiders—were selected based on their relevance and likelihood of exploiting the open server. Likelihood and severity scores were estimated based on threat motivations, attack history in similar organizations, and business impact. One limitation of this assessment is the lack of real-time monitoring data to validate assumptions.

Remediation Strategy

To reduce the identified risks, the company should restrict public access to the database using firewall rules and network segmentation. Implementing **multi-factor authentication (MFA)** and **principle of least privilege** will mitigate both external and insider threats. Regular audits and intrusion detection systems (IDS) should be deployed to detect unauthorized activities. These controls align with a **defense-in-depth** strategy and will significantly improve the system's security posture while supporting safe remote access for employees.