Vulnerability Assessment Report

Purpose

The database server is a critical asset for the company, enabling employees to query customer data remotely. Securing the data on the server is essential to maintain business continuity, protect sensitive customer information, and ensure regulatory compliance. If the server were compromised or disabled, it could result in significant business disruptions, loss of customer trust, and legal repercussions. This vulnerability assessment aims to identify potential risks and recommend controls to mitigate those threats effectively.

Risk Assessment

Threat Source	Threat Event	Likelihood (1-3)	Severity (1-3)	Risk (L x S)
Malicious hacker	Unauthorized access to customer data	3	3	9
Disgruntled employee	Data exfiltration	2	3	6
Competitor	Denial of service (DoS) attack	2	2	4

Approach

The selected threats represent realistic and potentially damaging attack scenarios. A malicious hacker is likely to target publicly accessible databases to steal valuable customer data. Disgruntled employees may exploit their privileged access to harm the company by leaking data. Competitors might resort to denial of service attacks to disrupt operations. These threats were prioritized due to their relevance, likelihood, and potential business impact.

Remediation

To mitigate these risks, the company should implement the principle of least privilege, ensuring users only have access to data necessary for their role. Multi-factor authentication (MFA) should be enforced to strengthen access security. Network access to the database should be restricted using IP whitelisting and VPNs. Monitoring and auditing user activity can also help detect and respond to suspicious behavior in real time.