Vulnerability Assessment Report

# Purpose

The purpose of this vulnerability assessment is to evaluate the security risks associated with keeping a remote database server open to the public. This server is critical for business operations, as employees worldwide rely on it to access customer data and identify leads. Protecting the confidentiality, integrity, and availability of the data is essential to maintain business continuity and customer trust. If the server were compromised or disabled, it could result in data breaches, regulatory violations, and operational downtime.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Source | Threat Event | Likelihood (1–3) | Severity (1–3) | Risk Score (LxS) |
| External hacker | Unauthorized access to customer data | 3 | 3 | 9 |
| Insider threat (disgruntled employee) | Data exfiltration or misuse | 2 | 3 | 6 |
| Cybercriminal group | Denial of Service (DoS) attack | 2 | 2 | 4 |

# Approach

The threat sources and events were selected based on their relevance to an exposed public database server. External hackers pose the highest risk due to the open nature of the server, increasing chances of unauthorized data access. Insider threats remain a concern for any organization handling sensitive customer data, especially with global remote access. Cybercriminals launching DoS attacks can interrupt operations, leading to significant business disruption and loss of customer trust.

# Remediation

To address these risks, several security controls can be implemented. Enforcing the principle of least privilege will reduce unnecessary access to the database. Deploying multi-factor authentication (MFA) can further secure remote logins. The organization should also move the database behind a secure VPN or firewall to limit public exposure. Additionally, regular auditing and monitoring using the AAA framework can help detect and respond to suspicious activity. These controls together can mitigate both external and internal threats while ensuring business continuity.