Vulnerability Assessment Report

Purpose

The database server is a crucial component of the company's operations, enabling employees to access and query customer information from remote locations. Keeping the database open to the public presents a serious security risk, as unauthorized users could exploit vulnerabilities to gain access to sensitive business data. Securing the server is essential to protect customer information, maintain business continuity, and comply with data protection regulations. If the server is compromised, it could result in data breaches, financial loss, reputational damage, and operational disruptions. This assessment aims to evaluate the risks associated with the open database and recommend security measures to mitigate these risks.

Risk Assessment

Threat Source	Threat Event	Likelihood (1-3)	Severity (1-3)	Risk Score (Likelihood x Severity)
Malicious Hackers	Unauthorized data access and exfiltration	3	3	9
Insider Threats	Accidental or intentional data leaks	2	3	6
Automated Bots/Scripts	Denial of Service (DoS) attack	2	2	4

Approach

The identified threats were chosen based on the system's vulnerabilities and potential consequences. Malicious hackers pose a significant risk due to the publicly accessible database, making unauthorized access and data breaches a critical concern. Insider threats, whether accidental or intentional, can lead to significant data leaks, impacting customer trust and business operations. Additionally, automated bots can exploit the open database by executing Denial of Service (DoS) attacks, potentially rendering the database inaccessible to legitimate users. These threats were prioritized based on their likelihood of occurrence and impact on business operations.

Remediation

To mitigate these risks, implementing security controls is essential. The **Principle of Least Privilege** should be enforced, ensuring employees have access only to the data necessary for their roles. **Multi-Factor Authentication (MFA)** should be required for database access to prevent unauthorized logins. **Defense in Depth** strategies, such as IP whitelisting, firewalls, and intrusion detection systems (IDS), can prevent external threats. Additionally, logging and monitoring mechanisms should be implemented to detect suspicious activities. By securing the database and limiting public exposure, the company can significantly reduce the risk of data breaches and cyber threats.
