Vulnerability Assessment Report

24st Sep 2025

System Description

The company's information system consists of a remote database server that stores critical customer and business data used by employees to identify potential customers. Since many employees work remotely around the world, the database has been left publicly accessible over the internet to allow direct queries. This setup allows for flexibility and ease of access, but it also exposes the database to significant security risks, such as unauthorized access and data breaches. The server is therefore a central component of business operations and requires robust security controls to ensure availability, confidentiality, and integrity of the data.

Scope

This vulnerability assessment focuses on the company's remote database server that has been publicly accessible since the organization's launch. The assessment evaluates the security risks associated with the server's exposure to the internet, including potential unauthorized access, data manipulation, and denial-of-service attacks. It also considers the impact such risks could have on business operations, customer trust, and regulatory compliance. The scope is limited to identifying vulnerabilities, assessing threat likelihood and severity, and recommending remediation strategies specific to the database server environment.

Purpose

The database server is central to the company's operations, as it stores valuable customer and business information that employees rely on to identify and serve potential customers. Protecting this data is critical to maintaining customer trust, ensuring compliance with data protection regulations, and safeguarding the company's reputation. If the server were compromised or disabled, the business could face operational disruptions, financial losses, and legal consequences. This vulnerability analysis aims to identify the risks associated with the exposed server and recommend actions to strengthen its security and resilience.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
1- External Hackers / Cybercriminals	*Attackers may exploit the public accessibility of the database to steal sensitive customer and business data, inject malicious queries, or disrupt services for financial or reputational gain.*	*3*	*3*	*9*
2- Malicious Insider	*A disgruntled employee or contractor with knowledge of the database structure and access methods could intentionally misuse credentials to extract, alter, or delete data.*	*2*	*3*	*6*
3-Automated Threats / Malware (e.g., Bots, Worms, or Ransomware)	*automated internet scans and malicious software could detect the open database and launch attacks, such as brute-force login attempts, SQL injection, or ransomware encryption of the stored data.*	*3*	*2*	*6*

Approach

In this qualitative vulnerability assessment, I selected three threat sources and related events that represent the most pressing risks to a publicly exposed database server. External hackers present a high likelihood of attempting a data breach, given that internet-facing systems are common targets for exploitation. Malicious insiders were considered because they often have privileged knowledge and access, making them capable of causing intentional data manipulation or deletion. Automated bots and malware were included due to their prevalence in scanning for exposed systems and launching denial-of-service attacks. These threats were

prioritized because each could significantly disrupt business operations, harm customer trust, and result in financial or regulatory consequences.

Remediation Strategy

To remediate the identified risks, the database server should be moved to a private network and access restricted using the principle of least privilege, ensuring only authorized users and applications can connect. Implementing multi-factor authentication (MFA) and the AAA framework will strengthen identity verification and accountability for administrative access. To mitigate insider threats and data manipulation, audit logging and monitoring should be enabled to detect unusual activity. Finally, applying a defense-in-depth strategy—including network segmentation, firewalls, and intrusion detection systems—will provide layered protection against external attacks such as denial-of-service attempts.