Vulnerability Assessment Report

Name: Hridhima Karmakar

System Description:

The system under review is a remote cloud-based database server that stores sensitive customer data for an e-commerce company. This server is accessed by employees from global locations and is currently open to the public internet, lacking authentication or access restrictions. The server plays a central role in daily business operations, including customer targeting, marketing campaigns, and order management. The attack surface includes remote access protocols, the database engine, user credentials, and internet-facing IP addresses.

Scope:

This assessment focuses on the confidentiality, availability, and integrity of data on the public-facing database server. It does not include the physical security of server hardware or unrelated IT systems. The goal is to identify risks stemming from unauthorized access and propose mitigation strategies that align with the organization's business and compliance goals.

Purpose:

The purpose of this vulnerability assessment is to analyze the risks associated with leaving the company's database server open to the public. This server is a valuable business asset that holds customer records and operational data, and its compromise could result in data breaches, downtime, and reputational damage. By identifying vulnerabilities and recommending security controls, this assessment aims to protect the company's data, maintain trust with its customers, and ensure the continuity of services.

Risk Assessment Table:

Threat Source	Threat Event	Likelihood (1-3)	Severity (1-3)	Risk Score (1-9)
External Hacker	Unauthorized access and data exfiltration	3	3	9
Insider Threat	Accidental or intentional data deletion	2	3	6
Competitor or Adversary	Denial of Service (DoS) attack	2	2	4

Approach:

The threat sources and events were selected based on the system's public exposure, operational importance, and potential exploitation methods. The lack of access controls makes the server highly susceptible to external attackers seeking to steal data. Insider threats, whether accidental or malicious, pose a real risk due to weak user permissions. Finally, the threat of service disruption through a DoS attack from competitors or adversaries could significantly impact service availability. These threats were prioritized based on their relevance, likelihood, and potential business impact.

Remediation:

To remediate these vulnerabilities, the organization should implement multi-factor authentication (MFA) and restrict public access to the database using firewalls and IP allowlists. Enforcing the principle of least privilege will ensure that users only have access to the data necessary for their role, reducing the risk of insider misuse. For enhanced protection, implementing a defense-in-depth strategy, including intrusion detection systems (IDS), database encryption, and regular access log monitoring, will help prevent and detect malicious activity. These measures will collectively reduce exposure to the identified threats and strengthen the system's security posture.