Vulnerability Assessment Report

1st January 20XX

System Description

The database server features a strong multicore CPU and 128GB of RAM. It runs the most recent version of the Linux operating system and includes a MySQL database management system. The server is linked via IPv4 and connects with other computers in the environment. Currently, the database is publicly available over the internet, allowing distant employees to run customer-data searches. SSL/TLS encryption is used during data transfer, however access to the server remains accessible to all external users, resulting in a huge attack surface.

Scope

This vulnerability evaluation focuses on the access controls for the publicly accessible database server. The scope encompasses potential hazards to the confidentiality, integrity, and availability of consumer and business data housed on the server. Physical security and other unrelated IT systems are beyond the scope. The examination spans the three-month period from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 outlines the process for calculating and awarding likelihood, severity, and total risk ratings.

Purpose

The database server is essential to the company's e-commerce operations since it stores client information and other business-critical records. Securing sensitive data is critical for preventing unwanted access, fraud, and data breaches. If the server went down or was compromised, staff would be unable to obtain client data, reducing productivity, company continuity, and consumer trust. This vulnerability assessment seeks to identify risks connected with the publicly accessible server and offer steps that will help the firm achieve its security and operational objectives.

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External attacker	*Unauthorized access to the public database*	*3*	*3*	*9*
Malware / cybercriminal	*Exfiltration of sensitive customer information*	*3*	*3*	*9*
Insider threat	*Unauthorized modification of database records*	*2*	*3*	*6*

Approach

I chose these specific dangers because the database server is publicly accessible, making illegal access and data theft the most serious concerns. Using NIST SP 800-30 Rev. 1, I assessed the likelihood and severity depending on the sensitivity of client data, the lack of authentication, and the server's public visibility. Scores were provided qualitatively, based on the realistic likelihood of assaults and their possible commercial impact. Limitations include little understanding of internal logging processes and insufficient visibility into present monitoring technologies.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

Remediation Strategy

To protect the server, the business should limit public access by installing a firewall, activating IP allow-listing, and mandating VPN authentication for all users. Applying the concept of least privilege ensures that workers only have access to the data required for their position. To prevent unwanted logins, all administrative accounts should have multi-factor authentication (MFA) enabled. In addition, frequent log checks and database auditing should be undertaken to detect any unusual behavior. Implementing these measures will dramatically minimize the likelihood of illegal access, data loss, and service disruption.

Consider the following questions to help you write a remediation strategy:

- *Which technical, operational, or managerial controls are currently implemented to secure the system?*

- *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*
- *How will the results of the assessment improve the overall security of the system?*