Scenario Overview

This report is based on a mock cybersecurity exercise, designed to evaluate security vulnerabilities in an e-commerce company's database infrastructure. The company operates with a remote workforce and relies on a publicly accessible database server for business operations. However, public access to the database introduces serious security risks, including unauthorized access, data breaches, and operational disruptions. This assessment follows the NIST SP 800-30 Rev. 1 guidelines to identify, assess, and mitigate these vulnerabilities.

Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

- The database is fundamental to the company's operations, enabling employees to retrieve and analyze customer data. However, its public accessibility poses a significant security risk. Unauthorized access could lead to data breaches, operational disruptions, and financial loss. If the database were compromised, attackers could steal or alter sensitive customer and business information, impacting both the company's reputation and compliance with data protection regulations. This vulnerability assessment aims to evaluate these risks and propose security measures to protect critical assets.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Cybercriminals	*Steal sensitive data for ransom or sale*	*3*	*3*	*6*
Competitors	*Competitors having access to private company data that could lead to an unfair competitive advantage*	*2*	*3*	*5*
Insider Threat	*Data manipulation (tempering or removing data to disrupt operations), distribution of sensitive data*	*2*	*3*	*5*

Approach

The threats assessed represent the most immediate and likely vulnerabilities that must be addressed. Cybercriminals actively seek exposed systems to exploit for financial gain or to disrupt operations, and a publicly accessible database creates an easy entry point for malicious actors. This significantly increases the risk of unauthorized access, data exfiltration, and system compromise. A potential data breach not only poses a severe reputational risk but also exposes the company to financial penalties and legal consequences due to non-compliance with security regulations. Securing this database is critical to mitigating these risks and ensuring business continuity.

Remediation Strategy

It is imperative that the company takes immediate action to remediate these vulnerabilities. During this assessment, our team identified key security measures that must be implemented to protect both customer and business data.

- **IP Allow-Listing:** Restrict database access to a predefined list of trusted IP addresses, ensuring that only authorized employees and systems can connect. This reduces the risk of unauthorized external access.

- **Authentication & Logging:** Implement strong authentication mechanisms, such as Multi-Factor Authentication (MFA), to verify user identities. Additionally, enforce access logging to track who accesses the database, when, and from where, providing valuable audit trails for security monitoring.
- **Authorization & Least Privilege:** Apply the Principle of Least Privilege to ensure that users have only the minimum necessary access required to perform their tasks. Role-Based Access Control should be enforced to prevent unauthorized data exposure.

These measures will address the immediate vulnerabilities; however, ongoing security assessments, periodic audits, and additional security layers—such as encryption and intrusion detection—should be implemented to further enhance database protection over time.