Vulnerability Assessment Report

1st January 20XX

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

A vulnerability assessment of the situation can help you communicate the potential risks with decision makers at the company. You must create a written report that clearly explains how the vulnerable server is a risk to business operations and how it can be secured.

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

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?*

The purpose of the database server lies in its pivotal role in facilitating efficient business operations. Its value is underscored by its function as a repository of crucial business data, enabling informed decision-making and streamlined processes. Securing the data on the server is paramount to safeguard sensitive information, maintain regulatory compliance, and uphold customer trust. In the event of server incapacitation, the business could experience severe disruptions, hampering productivity, customer service, and revenue streams. Hence, ensuring the robustness and security of the database server is imperative to sustain business continuity and resilience.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Malicious Software	*Disrupting operations and facilitating unauthorized access*	*3*	*3*	*9*
Temperature controls	*Equipment, data loss, or service disruptions*	*2*	*2*	*4*
Hacker	*Encompass unauthorized intrusion, data breaches*	*3*	*3*	*9*

Approach

The selection of these specific threat sources/events is rooted in their potential to significantly impact business operations and overall security. Malicious software presents a high likelihood of disrupting operations and enabling unauthorized access, which can cripple business continuity and compromise sensitive data. Temperature control issues, though less likely, can lead to equipment failure, data loss, or service interruptions, causing disruptions and potential financial losses. Hackers, with their ability to execute unauthorized intrusions and data breaches, pose a severe risk to both data integrity and customer trust, warranting substantial concern. The assigned likelihood and severity scores highlight the notable risks these threats pose, emphasizing the need for comprehensive mitigation strategies.

Remediation Strategy

To effectively address the identified risks within the target system, the vulnerability assessment report advocates a comprehensive approach to security. Implementation of the principle of least privilege can significantly mitigate threats by limiting user access to only necessary resources, curbing potential unauthorized activities. The defense-in-depth strategy involves layered protective measures, bolstering the system's resilience against various attacks. Multi-factor authentication (MFA) offers an extra layer of defense by requiring multiple verification factors for user access. Furthermore, adopting an Authentication, Authorization, Accounting (AAA) framework enhances control over user actions and enforces accountability. These security controls collectively contribute to a robust mitigation and remediation strategy, enhancing the system's overall security posture.