Vulnerability Assessment Report

1st January 2024

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 2024 to August 2024. 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:

- The MySQL database server is a critical asset for the business, supporting operations by storing and managing valuable customer and business data. Securing this data is essential to protect the organization from data breaches, regulatory penalties, and loss of customer trust. Public accessibility of the server poses significant risks, including unauthorized access, data theft, and malicious attacks. If the server were compromised or disabled, the business could experience operational disruptions, financial losses, and reputational damage. This vulnerability analysis aims to identify these risks and recommend measures to secure the server, ensuring business continuity and data integrity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Unauthorized access*	*3*	*3*	*9*
Employee	*Accidental malware introduction*	*3*	*2*	*6*

Competitor	*Collection of business data for competitive use*	*2*	*3*	*6*

Approach

This vulnerability assessment focuses on three critical threat sources: malicious hackers, business competitors, and internal employees. These were selected as they represent the most probable and impactful risks due to vulnerabilities within the company, such as a publicly accessible database and remote workforce. The identified threat events: unauthorized access, accidental malware introduction, and collection of business data for competitive use are considered significant because they could lead to severe financial losses, reputational damage, and major business disruptions, as displayed in the risk analysis chart.

Remediation Strategy

To address the identified risks, the following security controls are essential. Since employees work remotely, their risk of malware exposure increases; therefore, **security awareness training** is crucial especially for social engineering tactics. To prevent unauthorized data collection and other outside threats, we must implement the **AAA framework**. This includes **multi-factor authentication** to verify user identities and the **principle of least privilege** to ensure users only access necessary data for their specific job functions. Finally, the MySQL database should be configured to trace user activity, providing an essential audit trail for forensic analysis.