Vulnerability Assessment Report

8 September 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

The database server is a critical asset for the company as it stores essential business information, including customer data, which is publicly accessible. Securing this data is vital to protect the company from malicious actors who might exploit the information for various purposes, potentially harming the company's reputation, client privacy, and financial standing. If the server were compromised or disabled, it would disrupt business operations, leading to data loss or theft, operational downtime, and the exposure of sensitive information to unauthorized access. Such an event could result in severe reputational damage and financial losses.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External Hacker	*Data exfiltration via malware*	*3*	*3*	*9*
Insider (Employee)	*Alter critical information in the database*	*2*	*2*	*4*

APT/Nation-State Actor	*Denial of Service (DoS) attack*	*3*	*3*	*9*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Remediation Strategy

User Access Controls: Set up strong rules to make sure only the right people can access the database server. This includes using strong passwords, giving users access based on their job roles, and requiring a second form of verification (like a code sent to their phone) to log in.

Data Encryption: Protect data while it's being sent by using the latest encryption methods (such as TLS 1.3). This ensures that sensitive information is safe as it travels between users and the server.

Network Security: Limit who can access the database by allowing only specific IP addresses from trusted locations, like company offices. This helps block unwanted access from the outside.

Monitoring and Alerts: Set up a system that constantly checks for unusual activity and sends alerts if anything suspicious happens. This allows for quick responses before any potential issues become bigger problems.