Vulnerability Assessment Report

30th 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 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:

Value to the Business: The database server is crucial for efficiently storing, managing, and retrieving vital business information, such as customer records, sales data, and inventory levels. This centralized data management streamlines operations and supports informed decision-making, enhancing overall productivity.

Importance of Data Security: Securing the data on the server is essential to protect sensitive information from breaches and cyberattacks. Data loss or unauthorized access can lead to financial losses, legal repercussions, and damage to the business's reputation. By implementing strong security measures, the business safeguards its assets and builds trust with customers.

Impact of Server Downtime: If the server were disabled, the business could face significant disruptions. Operations reliant on the database, such as order processing and customer service, would be severely affected. This could lead to lost sales, dissatisfied customers, and hindered business growth. In severe cases, extended downtime could jeopardize the business's viability.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Threat Actors	*This includes malware, ransomware, and hacking attempts that could compromise data integrity and confidentiality. Attackers may exploit vulnerabilities in the operating system, database software, or network configurations.*	*3 (Cyber attacks happen often and are always evolving)*	*3 (A successful attack can result in significant data and financial loss)*	*3*
Insider Threats	*Employees or contractors with access to the server may intentionally or unintentionally cause data breaches or system misconfigurations. This risk is heightened if proper access controls and monitoring are not in place.*	*2*	*3*	*2*
Network Security Issues and Misconfigurations	*Weaknesses in the network infrastructure, such as unprotected endpoints or insecure protocols, can lead to unauthorized access or data interception. Ensuring strong network security measures are in place is essential to prevent these risks.*	*3*	*2*	*2*

Approach

My approach to classifying risks and vulnerabilities within this information system incorporates a comprehensive analysis of various factors, including Common Vulnerabilities and Exposures (CVEs) and the prevailing trends in cyber attack methodologies. This holistic perspective allows for a more accurate assessment of potential threats and their impact on the system's security posture.

Remediation Strategy

My recommendations for remediation include maintaining up-to-date software and operating systems, implementing consistent monitoring of network traffic to detect anomalies, and investigating any suspicious activities. Additionally, I advocate for employee education on the risks associated with social engineering and the various tactics employed by threat actors. This

multi-faceted approach will enhance the overall security posture of the organization.motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.