Vulnerability Assessment Report

20th 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 October 2023 to December 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server holds customer credentials and sensitive business information, which must be safeguarded from public access. Unauthorized access to this information could have severe implications for the organization, leading to compliance issues, financial losses, and reputational damage if exploited by threat actors.

Securing data on the server is crucial for any business, given that servers store both customer and sensitive business information. Leaving the server unprotected makes it vulnerable to attacks, and threat actors often specifically target organization servers as they house valuable data. Since servers contain information critical to the organization, ensuring their security is paramount to prevent exploitation by malicious actors.

The unavailability of the server to authorized users would impede business operations. A potential data breach could result in a breach of confidentiality, leading to financial losses, reputational damage, and a loss of customers' trust and confidence.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hackers	*Obtain sensitive information when they exploit the server.*	*3*	*3*	*9*
Hardware	*Unavailability of data due to server failure.*	*3*	*2*	*6*

Approach

My rationale for selecting the three threat sources is based on their likelihood of occurrence and the significant impact they pose to the organization. Competitors, aiming to gain a market advantage, pose a major threat by potentially disrupting the organization's operations, rendering it unavailable to customers. Hackers, driven by an interest in sensitive information, particularly focus on exploiting servers holding valuable data, leading to financial losses and compliance issues upon unauthorized access. Additionally, hardware failures are inherently probable, and without resilient measures to maintain server availability, the organization may face disruptions, impacting its accessibility to authorized users.

I assigned likelihood and severity scores to the mentioned threats based on their historical occurrences and the resultant damage observed in other organizations. Considering the competitive landscape, where each competitor seeks a market advantage, disruptions to our operations are highly likely. Hackers, driven by specific interests, consistently attempt to exploit our organization's data, posing a significant threat. While hardware failure is more probable, its impact is not severe, mainly causing an unavailability of server access for authorized users.

The assessment was constrained to a three-month period due to limitations in time, which proved insufficient for a comprehensive exploration of information. Additionally, the available resources for the assessment were inadequate, further restricting the depth and breadth of the evaluation.

Remediation Strategy

The system is equipped with a configuration of rule sets governing incoming traffic to restrict direct access. Staff undergo annual training to enhance awareness of potential cyber threats, and various policies, including access control and password policies, are in place to ensure comprehensive security measures.

While existing security controls are in place, the organization should contemplate enhancements to its policies. Implementing rule sets for outgoing traffic is vital to prevent unauthorized data exfiltration. Employees should undergo training at least quarterly to foster a deeper understanding of common vulnerabilities. Additionally, a regular quarterly review of policies is recommended to identify and address any disclosed vulnerabilities, along with the implementation of an account usage policy for comprehensive security measures.

The assessment results will contribute to enhancing the overall security of the system by enabling swift and targeted responses. The organization should persist in regularly evaluating its risks and monitoring the mentioned threat sources to ensure an ongoing and proactive approach to security management.