Vulnerability Assessment Report

15th September 2023

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 2023 to August 2023. 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 database server–a centralized system–is valuable to the business because it serves as a repository and manager of a large amount of data and its services are regularly used for marketing operations. More specifically, this server is utilized for storing customer details, campaign information, and analytical data, which proves valuable for the company's marketing efforts because it can be used for subsequent analysis of performance tracking and personalized marketing endeavors. Consequently, the business would find it important to secure the data on the server because of its capacity to convert potential customers into actual ones, potentially leading to increased profits. As a result, if this server were to be disabled, it could impede sales and jeopardize the overall functionality of the company.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Threat source	Threat event	Likelihood	Severity	Risk
Employee	Interrupt essential operations	2	3	6
Hacker	Acquire sensitive information through unauthorized extraction	3	3	9
Customer	Modify/Erase critical information	1	3	3

Approach

Evaluated risks took into account the business's data storage and management procedures. Identification of potential threat sources and events was based on the probability of having a security incident, considering the open access permissions of the information system. The severity of potential incidents was assessed in relation to the impact on daily operational requirements.

Risks were assessed by considering the data storage and management approaches employed by the business. The likelihood of threat occurrences and their potential impact were compared against the risks posed to daily operational needs.

Remediation Strategy

Enforcing authentication, authorization, and auditing mechanisms is imperative for restricting database server access to just authorized users. This involves implementing

such robust security measures as strong password protocols, role-based access controls, and multi-factor authentication to limit user privileges. Additionally, data in motion is secured through TLS encryption rather than SSL. IP allow-listing is also implemented, thus restricting database server access to just the corporate offices.

To prevent unauthorized connections to the database server from the internet, it is essential to employ Identity and Access Management (IAM) for the database. Mitigating such risks also involves using such approaches as the principle of least privilege and eliminating public access altogether. Lastly, distributing the database across multiple regions will minimize the likelihood of a natural disaster causing a system outage.