Renaldo Schmidt

Vulnerability Assessment Report

1st September 2023

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of the 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

- The server is valuable to the organization because it lists potential customers, which could lead to sales.
- It is important for the business to secure that data on the server because competitors can steal our potential customers. Also, if the data were to be lost or corrupted due to an attack, then we would lose potential customers.
- If the server were to be disabled, then the business would lose its main source of leads, which would negatively impact sales.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	3	2	6
Hacktivist	Alter/Delete critical information	1	3	3
Communications	Conduct Denial of Service (DoS) attacks	1	2	2

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. The business is at the biggest risk of a competitor stealing our potential customers because this is the most likely event to occur, and it would lead to a loss of sales. The other two risks outlined are a hacktivist deleting our list, and a communications error with the server due to a DDoS attack. These are not as big of a risk, but if they were to occur, then we would also lose sales.

Remediation Strategy

I recommend the implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.