Vulnerability Assessment Report

30th 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 June 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this vulnerability assessment is to show why having the company's database open to the public for the last three years is detrimental to the company. The database hosts all our customer information and our business trends. Leaving this open to the public allows our competitors to potentially obtain customers that would have been ours if our database was not open to the public.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Install persistent and targeted network sniffers on organizational information systems*	*3*	*3*	*9*
Disgruntled	*Alter/Delete critical information*	*2*	*3*	*6*

former employee				

Approach

The thought process behind each risk of either a competitor, hacker, or a former disgruntled employee is that with a public server human interferences are at a higher risk due to availability. A competitor and a hacker would find obtaining information or placing a virus/malware soft too tempting of a chance to avoid. A disgruntled former employee is the least likely to happen due to the nature of our offboarding process.

Remediation Strategy

My recommendations for remediation to prevent this issue from persisting is to make our server private for only our employees to access, implement a proper authentication and authorization process for employees, and place the proper prevention and detection tools for information security.