Vulnerability Assessment Report

1st February 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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database holds valuable customer information vital to the company's existing and new business. It is important to secure the data and the database system. Not only should the data be restricted access but allowing the system to be public leaves the data open to manipulation by outside threats. Having the server open to the public allows an open door to malicious threat actors who may wish to attack other parts of the company's digital infrastructure.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Theft or Destruction of company infrastructure.*	*3*	*3*	*9*
Competitor	*Theft of Data or Access to information that may threaten company market share and ability to compete.*	*3*	*2*	*6*

System Administrator	*Public access to the database risks a lateral attack on the system administrator and may further risk other related systems and data like customer information or financial information.*	*3*	*3*	*9*

Approach

Although I have selected three examples in my analysis of risk, the severity of the vulnerability leaves the company open to many unwanted consequences like data loss, damage to company equipment as well as lawsuits from customers and fines for violation of regulations and lack of compliance. Because the database and the company network and infrastructure are so exposed, the likelihood and severity of an attack in almost any case are quite high.

Remediation Strategy

While the vulnerability of the database is severe, there are a few controls and practices that can be implemented quickly and affordably. Because many employees access the system remotely, all employees should be assigned appropriate access to the database and files through management of permissions. A VPN should also be used by any employee accessing the system remotely. Multi Factor Authentication will help add another affordable layer of security. Taking these three steps will greatly reduce the likelihood of an attack.