Vulnerability Assessment Report

1st 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 assessment is to analyze the current state of access controls on the remote database server. Company's employees regularly query data from the database server to find potential customers, making the database a highly valuable asset in addition to containing customer's personal information. Securing the availability of the database is crucial to the business for uninterrupted operations and safeguarding sensitive information.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Alter/Delete critical information*	*1*	*3*	*3*
Hacker	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*

Approach

The database has been open to the public since the company's launch three years ago. A business competitor could easily steal customer information to their advantage. Because the database is open to the public, a hacker might more easily be able to launch a Denial of Service (DoS) attack. An employee may make modifications to critical data by mistake, which is a less likely but nonetheless relevant threat.

Remediation Strategy

The security team suggests the implementation of authentication, authorization, accounting (AAA) framework to only allow access to authorized personnel. Multi-factor authentication (MFA) can also be added to the authentication stage by requiring the user to enter more information than just a password. After the users are authenticated and authorized, they must be monitored in order to track who accessed, when they accessed and what resources they used. To reduce the mistakes of modifying critical data, a principle of privilege method must be put in place to give users only the necessary permissions to do their task.