Vulnerability Assessment Report

1st May 2023

System Description

The server is a powerful computer with a fast processor and a lot of memory (128GB). It uses the latest version of the Linux operating system and hosts a system for managing databases called MySQL. It's connected to the network using regular old IPv4 addresses and communicates with other servers on the network. To keep things safe, it uses SSL/TLS encryption for secure connections.

Scope

This report looks into how secure the system is in terms of who can access it. We're checking over a three-month period, from June to August 2022. We're following guidelines from NIST SP 800-30 Rev. 1 to help us analyze the risks to the system.

Purpose

The database server is like a big information storage place. It keeps lots of data, including stuff about customers, marketing campaigns, and analysis. This data helps us see how things are going and plan our marketing. It's really important to keep this system secure because we use it a lot for our marketing work.

Risk Assessment

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

Approach

We looked at how the business stores and manages data and figured out what could go wrong. We thought about where security problems might come from and how likely they are given how open the information system is. We also looked at how bad things could get if these problems actually happened.

Remediation Strategy

To make things safer, we'll put in place some measures. We'll make sure only authorized people can access the database server. This means having strong passwords, giving people access based on their roles, and making them use two or more ways to prove they are who they say they are. We'll also use TLS to encrypt data that's moving around and be careful about who we let connect to the database server from the internet. We'll mostly limit it to people in our corporate offices to keep things secure..