Vulnerability Assessment Report

1st January 20XX

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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is incredibly valuable to the business as employees around the world regularly query and request data from it. The server stores analytic and customer data used for marketing. It is used to find potential customers, track performance and trends and is a source of information for employees. It is important to secure this as if information was changed, leaked or disabled it could cause disruptions in business operations, harm to company reputation or regulatory risks.

Risk Assessment

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

Approach

My rationale behind choosing these 3 threats was because of the scope of the assessment. As the scope was focused on access controls, I wanted to focus on who had potential access and what would happen if that access was mismanaged or broken by the wrong people. Insiders are more likely to have access and then mismanage it than outsiders, but the problem is that the database has apparently been public since the company's launch. This means that all access control events have a higher likelihood but those don't by malicious threats will always have a higher severity and may be harder to remedy than those done by a non-malicious employee. The limitations were a lack of information and the limits of the scope being focused on access controls.

Remediation Strategy

I would recommend making access to the database based on a need-to-know basis using the principle of least privilege. This way only employees who need access for their jobs will be able to access the database and those who only need to read or query the database will not have permission to edit it, reducing the risk of accidental deletions or changes. It will also be easier to track changes made as only those who need permission to change information will be able to do so. It also reduces the risk of outside threats as if an employee's workstation gets compromised, the damage they can do will be limited by their permissions. The database should also be put behind an AAA framework where users need to authenticate themselves first before gaining access to the information they're authorized to have access too. By removing the database from a public view and limiting permissions this way it makes it harder for outside and inside threats to disrupt business operations.