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 server is extremely valuable to the company because it stores and manages data. This specific server is used to store information such as customer data, campaign information, and other analytics. If data is not properly secured and stored on this server it is at risk of being attacked by potential attackers or manipulated for malicious purposes.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Steal information to try and exploit weaknesses in the company*	*2*	*3*	*6*
Hacker	*Steal important data*	*3*	*3*	*9*
Employee	*Disrupt the flow of company operations from inside the company grounds*	*2*	*3*	*6*

Approach

I considered these 3 specific risks because I felt that they were the most common ones to occur based on company operations and standards. Competitors will always do what they can to gain an edge on competition even if it's through unethical practices. Hackers are a common threat actor when it comes to stealing information from data servers. Lastly, having a company puts you at risk from potential insider attacks which is why I selected “employee” as my final threat source.

Remediation Strategy

The remediation strategy should be to make sure all data is encrypted properly and stored safely and in secure locations. The principle of least privilege should be applied and all user permission should be managed and up to date with company standards. MFA should also be used to ensure that customer data is much harder to access from vulnerabilities such as weak passwords.