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

Consider the following questions to help you write:

A database server is very important and valuable to a business because it's the location where all sensitive information and data is held. With these large amounts of data not being secured, anyone can access this information. This can result in people using this information with malicious intent to blackmail our company for leaking sensitive information. This database is used by our company for daily operations, therefore with no database available to use the company would have to stop operation until further notice. Resulting in money being lost.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Alter/deleting critical information*	*3*	*3*	*9*
Employee	*Install persistent and targeted network sniffers on organizational information systems.*	*2*	*2*	*4*

Business partners	*Craft counterfeit certificates*	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.