

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:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The purpose is to evaluate the current access controls of the systems, because it is key to maintain the business operation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
<i>E.g. Competitor</i>	<i>Obtain sensitive information via exfiltration</i>	<i>1</i>	<i>3</i>	<i>3</i>
<i>Hacker</i>	<i>Obtain full access to the database</i>	<i>3</i>	<i>3</i>	<i>3</i>
<i>Privileged user</i>	<i>Having no control</i>	<i>2</i>	<i>3</i>	<i>3</i>

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.

The database is open to the public and that's a serious vulnerability easy to exploit.

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.

Having the database close to the public is a must and, in top of that, implementing measurements like the Least Privilege Principle, MFA and the AAA framework.