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?*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Dos attack	*The database is public, threat actors would see the sensitive information on it and bring the server offline, probably ceasing business operations.*	*1*	*3*	*3*
Threat actor	*Accessing confidential client PII or SPII through a publicly accessible database, could lead to identity theft.*	*3*	*3*	*3*
Employee/insider	*Altering of client records or data*	*2*	*3*	*3*

threat	*form low level employees who have too much access to data they do not need.*			

Approach

My explanation for the specific attacks are as follows, DDos would bring the server offline and compromise the accessibility of the service we provide to the client and halting business.

Threat actors having access to the database is a big issue since it violates the principle of confidentiality, our clients PII and SPII could be used for malicious intent such as identity theft, this could also possibly violate PCI DSS incurring heavy financial penalties.

Employee/insider threat this could lead to the compromise of client data integrity as employees in this company do not have a policy of least privilege they are adhering to. This means that they can alter/access data they have no need to see nor touch, this would negatively impact company reputation.

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. Least privilege security measures should also be implemented as well as setting the server to private. A backup of this server would also be a good measure as the data in this one is now known and is a risk now that potential threat actors know valuable information is on it. Proper firewall implementation and configuration would also be an asset to minimize the surface of attack for possible Ping, smurf, (D)Dos attacks.