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?*
    - Database server was used by employees working remotely to be able to access information on "potential customers" as stated in the scenario and was made publicly accessible since launch to allow ease of use,
- *Why is it important for the business to secure the data on the server?*
    - The server holds information on customers which could potentially include sensitive information such as PII or SPII. The server is used for e-commerce meaning the information may also include credit card information and transactions which must follow compliance and regulations in order to avoid financial costs to the business.
- *How might the server impact the business if it were disabled?*
    - Loss of the server would hurt business continuity and may also affect customer trust in the company as service is halted, slowed or may more negatively affect customers indirectly.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Obtain stolen sensitive information to sell of commit identity theft*	*3*	*3*	*9*
Networking	*Communication with other servers could serve as an attack surface for malicious attacks*	*2*	*3*	*6*

Approach

The server is most likely used for financial transactions and storage or sensitive information on customers and their transactions. It is highly likely that this asset will be targeted by competitors and hackers, given the nature of the server being open to the public and not protected behind multiple layers of defense as recommended by OWASP's defense in depth security principle. The opportunity also presents itself, again, with the server being allowed to communicate with other servers openly due to employees needing remote access to work. Adding networking traffic to the server as another attack surface for threat actors to use

Remediation Strategy

Recommendation for improved security and addressing vulnerabilities:

- Principle of least privilege
    - This will allow employees to access the server for the need to do their work, and removes the need for the public to have access to the server
- Defense in depth
    - Protects the server from malicious actors with more layers of security, this will meet compliance requirements as well as improve customer trust in the company with their data being kept private and secure.
- Multi-factor authentication (MFA)
    - This will strengthen the security of the server by making remote access to the server require more authentication, this will require attacks to do more work to gain access to the server whereas employees will be easily authenticated due to having a One-Time-Password or stored biometric information.

- Authentication, Authorization, Accounting (AAA) framework
    - This framework will help in the over security of the server by implementing more OWASP security principles such as Separation of duties