**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](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The MySQL database is connected to several servers, houses SPII, and is accessible by the public. The server is not secured at all and if it were to be attacked it could likely shut the company down for good. Given that the company is an E-commerce company there are higher than normal risks given the financial nature of the business.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *2* | *3* | *6* |
| *Hacker* | *Obtain sensitive information via exfiltration* | *2* | *3* | *6* |
| *Malicious software* | *Alter/Delete critical information* | *1* | *3* | *3* |

# Approach

This business is an E-commerce business and conducts business dealing with various sums of money. E-commerce is also a competitive field and involves lots of money. Given this the main factors it needs to be concerned with in this scenario is Competitors stealing or deleting information in order to close the company down or hurt their business and hackers looking to steal the information to use or sell. This also includes malware that could aid in either of these things.

# Remediation Strategy

Given that the server is open to the public the first stop is to lock it down using access controls. Requiring all remote workers to use a VPN to access the server will ensure the data in transit is encapsulated and encrypted in addition to PKI. The biggest vulnerability of this server is being remotely accessed; these two steps are vital to ensure confidentiality, integrity, and accessibility of the SPII located on the server. Other things to implement are:

* All employees must now use MFA and a password of at least eight characters, at least one uppercase, at least one lowercase, and at least one number.
* Role-based access control, only giving access to the server to those in the company who actually need the access.