**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

Consider the following questions to help you write:

*A vulnerability assessment is necessary to ensure the availability of the server containing all the information necessary for the company to conduct its operations. The security of the server is important so compliance like PCI DSS, GDPR regulations are not violated. If the server is disabled the business cannot run due to it being the center of operations.*

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | Perform reconnaissance and surveillance of organization | *1* | *2* | *2* |
| *Employee* | Alter/Delete critical information | *2* | *3* | *6* |
| *Hacker* | Craft counterfeit certificates. | *3* | *3* | *9* |

# Approach

Competitors can spy on the organization in a bid to have access to marketing strategy or products in development to gain an unfair advantage. Disgruntled or morally compromised employees can alter records to perform or cover up details of a crime. A hacker can also want to gain access to the company’s database to steal PII and SPII. To do this they may gain the trust of the server by crafting counterfeit certificates.

# Remediation Strategy

To prevent parties like competitors to gain access to the server a firewall IP whitelist must be maintained. The connection should also be encrypted with the latest encryption standards.

The principle of Separation of duty should be implemented to mitigate against employee fraud. Any one who enters data should not have access to alter the data.

Latest versions of TLS/SSL should be implemented while the base configurations should follow a standard protocol. Regular vulnerability assessments of certificates and encryption should also be carried out and referenced to the CVE list.