**Vulnerability Assessment Report**

**1st January 2025**

# **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 2025 to August 2025. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

Consider the following questions to help you write:

*The purpose is to assess this server for assurance that compliance is correctly implemented, because this asset contains PII from potentials customers and the data hosted here is important for making decisions. It is imperative protected and limited access to this server if not secured will affect the company reputation and would significate monetary losses.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Misconfigured server* | *Misconfigured services and protections on server could be a weakness* | *3* | *3* | *9* |
| *Power Outages* | *Corruption data when the electricity is not regulated* | *1* | *2* | *2* |

# **Approach**

*The logic for selected the risk that I evaluated is based on NIST SP 800-30, even the simplest and low priority can be the difference always thought random situations, for calculating score for each risk the values are since major number to low number where the 3 is Hight, 2 for Moderate and 1 Low, after decide likelihood and severity score will be multiplicate, the result will be risk score. I found limitations when I made this evaluation, little or scarce information about where the physical servers can be limited to add more environment threat sources as an example, we don’t know who can enter to servers’ room, CPU model, motherboard model, energy supply, etc.*

# **Remediation Strategy**

I recommend implementing the next policies :

* Setting up **Identify and Access Management**: Organized and classification who can access all data is the first layer to differentiate internal members and externals, like third partners or customers.
* Installing Operating System updates and services: Automatic updates always is a good choice to reduce the risk of weakness effectively.
* Implementing Multi-Factor Access: this recommendation is part of IAM, benign the second layer of access in this way we can assure that whoever try connecting to database really be who says are.
* Implementing password policies: defining a password policy would be a great plus to security.

After making the recommendations we can see how the use of CPU and RAM in the server will decrease, and just the employees can manipulate all data hosted in the server.