**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/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

*The database server is the only way for the business to continue it’s operations normally without the database server normal business operations would not be possible, It’s very important to secure the data on the server because it contains sensitive information most likely about the business and its customers.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hackers* | *Conduct Denial of Service (DoS) attacks.* | *3* | *2* | *6* |
| *Advanced persistent threat (APT)* | *Install persistent and targeted network sniffers on organizational information systems.* | *3* | *3* | *9* |

# **Approach**

*The reason I chose these risks is because outsiders are unpredictable they will attack you with all sorts of attacks, the reasoning of the likelihood and severity scores is because these have the potential to disrupt normal business operations which will likely disable business operations, the limitations of this assessment is we are preparing for known attacks where we are guided by the NIST framework, we have no plans for a zero-day attack.*

# **Remediation Strategy**

*In terms of technical controls, establishing firewalls and disabling unused ports can be a way to prevent Denial of Service (DoS) attacks, operational controls can be established when either of these threats go through there would be planning involved, and for managerial controls this is where most of the risk management process and security program planning and implementation is included. These will improve the overall security of the system in a way where we can prevent these attacks in happening in the first place.*