**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 valuable to the business because it stores critical customer and business data that employees access regularly to find potential customers. Securing the data on the server is important to prevent unauthorized access, data breaches, and potential misuse of sensitive information. If the server were disabled, it could significantly impact business operations, leading to loss of revenue, customer trust, and legal consequences.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Launch a Denial-of-Service(DoS) attack* | *2* | *3* | *6* |
| *Insider* | *Unauthorized data modification* | *2* | *2* | *4* |

# **Approach**

*The risks were selected based on the potential impact they could have on the business operations and data integrity. The likelihood and severity scores were derived by considering the ease of exploitation and the critically of the business functions affected. For example, a competitor exfiltrating data has high likelihood and severity due to its direct impact on business competitiveness and confidentiality. The limitations of the assessment include the exclusion of physical security measures and potential future threats not currently evident.*

# **Remediation Strategy**

*To mitigate the identified risks, the following secuirty controls are recommended:*

1. ***Principle of least Privilege:*** *Restrict database access to only those employees who neet it for their job functions to minimize the risk of data exfiltration and unauthorized modification.*
2. ***Defense in Depth:*** *Implement multiple layers of security controls, including firewalls, intrusion detection systems (IDS), and regular security audits, to protect against DoS attacks.*
3. ***Multi-factor Authentication (MFA):*** *Enforce MFA for accessing the database server to enhance authentication security and reduce the risk of unauthorized access.*