**Vulnerability Assessment Report**

**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 as it stores critical operational and customer data, ensuring seamless business processes and service delivery. Securing this data is essential to maintain customer trust, comply with regulatory requirements, and prevent financial losses or reputational damage. If the server were disabled, business operations could halt, leading to significant downtime, loss of revenue, and potential legal consequences. This vulnerability assessment aims to identify and address risks to safeguard the server's integrity, availability, and confidentiality.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *2* | *3* | *6* |
| *Competitor* | *Conduct Denial of Service (DoS) attacks* | *1* | *3* | *3* |
| *System administrator* | *Alter/Delete critical information* | *2* | *3* | *6* |

# **Approach**

The three threat sources—hacker, competitor, and system administrator—were selected based on their potential to exploit vulnerabilities in the database server. Hackers pose a moderate likelihood of exfiltrating sensitive data, while competitors, though less likely, could severely disrupt operations via DoS attacks. Privileged users, like system administrators, present insider risks with significant impact. These threats were prioritized due to their alignment with the server's critical role and the potential business impact, ensuring resources are allocated effectively to mitigate high-risk scenarios.

# **Remediation Strategy**

To mitigate identified risks, implement the following controls:

Principle of Least Privilege: Restrict administrator access to minimize insider threats.

Multi-Factor Authentication (MFA): Secure login processes to prevent unauthorized access by hackers.

Network Monitoring Tools: Detect and block DoS attacks in real-time.

These measures will reduce vulnerabilities, enhance data protection, and ensure business continuity.