**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:

* *How is the database server valuable to the business?*
* *Why is it important for the business to secure the data on the server?*
* *How might the server impact the business if it were disabled?*

The database server is quite crucial to the organization since it holds valuable data that is essential for the smooth running of the company. the data on ther server holds sensitive information about the company, staff and customers. Any compromise of the data on this server or the access issues would certainly impact the privacy of the organization and customers’ data, damage the corporate reputation and cause financial losses.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| Employee | * Obtain sensitive information via exfiltration. * Alter/Delete critical information. * Obfuscate future attacks. | *1* | *3* | *3* |
| Hacker | * Conduct Denial of Service (DoS) attacks. * Obtain sensitive information via exfiltration * Perform reconnaissance and surveillance of organization | *3* | *3* | *9* |
| Power outages | * Disrupt mission-critical operations. | *1* | *3* | *3* |

# Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Disgruntled employees have the capability and opportunities to strike from within the organization, thus causing tremendous damage to the integrity of the resources. While the likelihood is low, the severity of such actions when occurred is always high due to the ready access they have. On the other hand, hackers are always on the prowl looking for opportunities to inflict damage on corporate resources and reputation. The possibilities of an external compromise are always high, and so are the severity and risks. Finally, all electronic devices run on power, hence, power supply is crucial to the smooth running of the operations.

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

Backup power supply is crucial for ensuring that power failure doesn’t disrupt operations of the resources. Second, constant audit and monitoring should be implemented and enforced to ensure that internal sabotage does not compromise organization’s data and resources. Similarly, both principles of least privilege and separation of duties should be constantly adopted to ensure internal users only have appropriate levels of access and cannot initiate major changes on their own. Finally, the organization security architecture should constantly adopt a security siege culture i.e. they should act as if they’re under constant attacks from hackers. This way, their security posture does not allow for any slip ups. To this end, security measure such as Principle of least privilege, defense in depth, multi-factor authentication (MFA) and the Authentication, Authorization, Accounting (AAA) framework (amongst others) should be enacted.