**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**

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?*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Standard user* | *Obtain sensitive information* | *2* | *3* | *6* |
| *Outsider* | *Conduct Denial of Service (DoS) attacks* | *3* | *3* | *9* |
| *Privileged user* | *Alter/Delete critical information* | *2* | *2* | *4* |

# **Approach**

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

* *What was your rationale for selecting the risks that you evaluated?*
* *How were you deriving the likelihood and severity scores of each risk?*
* *What were the limitations of the assessment?*

*In conducting the vulnerability assessment, the risks were selected based on their potential impact on the business operations and the likelihood of occurrence. Likelihood and severity scores were derived by considering factors such as the capabilities of potential threat sources and the potential impact on business functions. The assessment's limitations include the reliance on subjective judgment for likelihood and severity assessments and the potential for unforeseen vulnerabilities not covered in the assessment.*

# **Remediation Strategy**

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Consider the following questions to help you write a remediation strategy:

* *Which technical, operational, or managerial controls are currently implemented to secure the system?*
* *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*
* *How will the results of the assessment improve the overall security of the system?*

*In the current system, technical controls such as SSL/TLS encryption for network connections and access controls for database management are implemented. However, operational controls like regular security audits and employee training on data handling practices are lacking.*

*To reduce the identified risks, implementing multi-factor authentication (MFA) for database access and intrusion detection systems (IDS) to monitor for unauthorized access attempts can enhance security. Additionally, enforcing regular security updates and patches for the operating and database management systems can mitigate vulnerabilities.*

*Implementing these security controls will enhance the overall security posture of the system by reducing the likelihood of unauthorized access and data breaches. Regular security audits and employee training will also improve awareness and adherence to security best practices, further bolstering the system's defenses against potential threats.*