**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?*

*The server holds critical business data, which supports daily operations and strategic decision-making.*

* *Why is it important for the business to secure the data on the server?*

*It is vital to protect sensitive data such as customer information and financial records, preventing data breaches and ensuring compliance with regulations like PCI DSS and GDPR.*

* *How might the server impact the business if it were disabled?*

*Disabling the server could disrupt business continuity, leading to financial losses, reputational damage, and potential legal issues.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Malicious Software* | *Install Persistent network sniffers* | *2* | *2* | *4* |
| *Environmental Factors* | *Power outage disrupting operations* | *2* | *3* | *6* |
| *Internal User* | *Alter/Delete Critical information* | *1* | *3* | *3* |

# **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?*

*Risks were selected based on their likelihood of occurrence and potential impact, derived from* ***NIST SP 800-30****. The chosen risks represent both internal and external sources, as well as environmental factors.*

* *How were you deriving the likelihood and severity scores of each risk?*

*Likelihood and severity scores were determined using historical data, expert judgment, and* ***NIST SP 800-30****'s guidelines. High likelihood and severity indicate greater attention and prioritization in remediation efforts.*

* *What were the limitations of the assessment?*

*The assessment focuses only on access controls and may not capture hardware or other infrastructural vulnerabilities.*

# **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?*

*Maintain current SSL/TLS encryption standards for data transmission and ensure encryption at rest to protect sensitive information from unauthorized access or exfiltration.*

*Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect persistent sniffers or unusual network activities, mitigating the risk of network surveillance by malicious software.*

* *Are there security controls that can reduce the risks you evaluated? What are those controls and how would they remediate the risks?*

*Install uninterruptible power supplies (UPS) to mitigate the risk of power outages, ensuring operational continuity during unforeseen disruptions.*

*Implement role-based access controls (RBAC) and monitor privileged user activities to prevent accidental or intentional data alteration or deletion.*

* *How will the results of the assessment improve the overall security of the system?*

*The remediation strategies, if implemented, will significantly enhance the security posture of the server, reducing vulnerabilities to data breaches, operational disruptions, and unauthorized alterations. These efforts align with the guidance provided in* ***NIST SP 800-30 Rev. 1****, ensuring that potential threats are managed proactively and effectively​.*