**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?*

The purpose of this vulnerability assessment is to identify and mitigate security risks associated with the public accessibility of the company's database server. The database server is a critical asset, enabling employees to query data for identifying potential customers, which is essential to business operations. Securing the data is vital to protect sensitive customer and company information from unauthorized access or breaches. If the server were compromised or disabled, it could disrupt business continuity, result in financial losses, and damage the company’s reputation. This analysis will provide actionable recommendations to enhance server security and align with organizational goals.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| Competitor | Obtain sensitive information via exfiltration | 3 | 3 | 9 |
| Customer | Alter/Delete Critical information | 1 | 3 | 3 |
| Hacker | Conduct Denial of service attacks | 3 | 2 | 6 |

# **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?*

The risks evaluated in this assessment were selected based on their potential to significantly impact the business's operations, reputation, and data security. The rationale for selection included factors such as the database's accessibility to the public, the nature of data stored, and the presence of known threat sources like competitors, customers, and hackers.

The likelihood and severity scores were derived using a combination of the NIST SP 800-30 Rev. 1 guidelines, prior knowledge of threat behaviours, and expert judgment. Likelihood scores considered the intent and capability of the threat source, while severity scores measured the potential impact on business operations if the threat event were to occur.

The limitations of this assessment include the reliance on qualitative scoring methods, which may introduce subjectivity, and the scope's restriction to access controls, potentially overlooking other vulnerabilities. Additionally, the three-month assessment period may not capture long-term trends or emerging threats comprehensively.

# **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?*

To address the risks identified in this vulnerability assessment, the following recommendations are proposed:

1. **Implement Access Controls and Encryption**  
   Strengthen access controls by restricting database access to authorized users only. Use multi-factor authentication (MFA) to verify user identities. Ensure all data in transit and at rest is encrypted using robust protocols like AES-256. These measures reduce the risk of competitors exfiltrating sensitive information.
2. **Regular Data Backups and Integrity Checks**  
   Establish automated data backups and implement integrity checks to detect and respond to any unauthorized alterations. This control mitigates the risk of customers accidentally or intentionally altering or deleting critical information.
3. **Deploy a Web Application Firewall (WAF) and Rate Limiting**  
   Install a WAF to monitor and block malicious traffic targeting the server. Implement rate limiting to reduce the impact of denial-of-service (DoS) attacks by hackers. These technical controls ensure system availability and protect business operations.
4. **Conduct Continuous Monitoring and Audits**  
   Utilize intrusion detection and prevention systems (IDPS) for real-time monitoring of suspicious activity. Schedule regular security audits to identify emerging vulnerabilities and ensure compliance with best practices.
5. **Enhance Employee Awareness and Training**  
   Train employees on cybersecurity best practices, including recognizing phishing attempts and secure handling of sensitive data. Educated employees can help prevent inadvertent security lapses.

By implementing these recommendations, the system's overall security posture will improve, minimising risks to critical business operations. These measures are realistic and achievable within the outlined scope and will address the vulnerabilities effectively.