**Vulnerability Assessment Report**

**1st April 2025**

# **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 March 2025 to June 2025. [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 database is highly important to business as it stores data of the business such as products or web code, but also it contains mainly sensitive data from our users, such as PII, but also financial information such as credit card numbers SPII*

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

*It is important to secure the data not only to guarantee the privacy of the customer data, but also to keep a good performance for the companies itself.*

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

*If the server is disabled, the business would be freeze as there won**’t be any services running, neither any transaction would be done an users would worry about their data.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hackers group* | *Obtain or ransom sensitive data and sell it on dark web or ask a payment for release of data* | *3* | *3* | *9* |
| *Employee* | *Get sensitive data to use it in his favor and delete or change sensitive info* | *2* | *3* | *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.

* Risks that were measured consider the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents was weighed against the impact on day-to-day operational needs.

# **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 remediate the publicly accessible database, implement a virtual private network (VPN) for employee access, restricting direct external connections. Secure the database server with a strong firewall and intrusion detection system, limiting allowed IP addresses and monitoring for suspicious activity. Enforce strict user authentication with multi-factor authentication (MFA) and role-based access controls (RBAC) to ensure only authorized personnel can access relevant data. Regularly audit and patch the database server and its supporting systems to address known vulnerabilities.