**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" \l "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 aim of this report is to assess curent assets for vulnerabilities and address them with remediation*

*steps. Furthermore, the datbase contains valuable data which may inlude personal identifiable*

*information that if exposed by attackers means gaining access to data that they can modify or use for*

*their own advantage whether it be for financial gain or social engineering attacks.A DDOS attack*

*could also be likely where it would mean service disruption and an impact with business operations*

*halting production, impacting trust and reputation with clients as well as financial costs as well as*

*non-compliance with regulatory standards.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Alter and steal data* | *3* | *3* | *9* |
| *Malicious Software* | *Infiltrate system.* | *3* | *3* | *9* |
| *Storage* | *Miuse / abuse of data, no fault tolerance.* | *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?*

*Hackers pose a significant threat to any organisation whom will take advantage of any exploits for their gain. Once they have an open door to your system they can use malicious software to run code gain access using a high privilege user acount possessing full access causing damage to data.When it comes to storage there is no contingency approach if in the event data has been manipulated thre is no restoration mehanism for backing data that can be used to restore data to its previous state.*

*In terms of limitation there is no clear view of whether data is personal or sensitive, cannot determine inventory of all assets which would have been valuable to determine a hardened security approach. Thre is no information to detrmine th employee's level of access so in this case the assumption would b that vry has same access levels. The business impact would include the folowing:*

*- Halt in business operations.*

*- impact on reputation*

*- trust issues with clients*

*- financial penalties with regulatory authorities*

# **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?*

*As a remediation suggestions this is whatould be implemented:*

*- Encypt the data using PKI where key pairs can be adopted 1 to enrypt and 1 to decrypt.*

*- As well as password to authenticate consider using MFA which adds an additional layer of security.*

*- Apply principle of least privileged ensuring employees have minimum access to perform their tasks.*

*- Apply separation of duties avoiding multi levels of acess rights.*

*- For remote connetions consider adopting a VPN which would avoid data intrception from hackers.*

*- Consider use of a firewall allowing only required ports, recommend using next generation.*

*In justifying these measures these controls can help with the following:*

*- MFA would strengthen authentication if a hacker obtains a password as MFA randomly generates*

*new codes.*

*- separation of duties would preven a user for example modifying SQL data and also granting DB*

*access to anothr user.*

*- VPN adds remote acess security by encrypting data during connections to a system preventing*

*eavesdropping from unauthorized users.*

*- use of a firwall would allow system admins from blocking data from entering the intrnal network. By*

*using a next generation firewall it would perform data filtering and receive firmware updates*

*automtically by the vendor on the cloud.*