**Vulnerability Assessment Report**

**1st January 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 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**

*The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via ex-filtration* | *3* | *3* | *9* |
| *hacktivist* | Obtain sensitive information to damage the companies reputation | *2* | *3* | *6* |
| *Hacker* | sensitive information to damage the companies reputation or sale on the dark web | *2* | *3* | *6* |
| *Hardware failure* | *Loss of access to or corruption of data contained in the database* | *1* | *3* | *3* |
| *Disgruntle Employee* | *Remove/alter data due to greivence with the company* | *3* | *3* | *9* |

# **Approach**

*With out knowing any other information about the environment that the database servers currently runs in, this assumes that the a general level of standard security practices are in place for the network the organization is operating, like Defense in depth, etc. These suggestions are target the weakest area of security, the human factor. Ensuring that the proper controls are in place and working will ensure that the companies sensitive data is kept secure.*

# **Remediation Strategy**

*The following controls should be implemented for better operational oversight and securing the data stored on the database sever.*

1. Implement Authentication, Authorization, Accounting (AAA) framework for accessing the server and\or its data
2. Develop and implement Principle of least privilege based on role(s) in the organization.
3. Consider implementing Multi-factor authentication (MFA) for users performing admin level functions on the server or the database.