**Vulnerability Assessment and Remediation Plan for Secure Remote Database Access**

**3rd June 2024**

# **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 2023 to August 2023. [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 works as a centralized repository for storing and managing extensive data, including customer information, campaign details, and analytics. This data is critical for tracking performance and personalizing marketing efforts. Therefore, securing the system is essential to maintain the integrity and confidentiality of the data, ensuring the continuous and secure operation of marketing activities.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker, Malicious Actors* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |
| *Hacker, Malicious Actors* | *Conduct Denial of Service (DoS) attacks.* | *3* | *3* | *9* |

# **Approach**

The assessment measured risks by examining the company’s data storage and management procedures. Potential threat sources and events were identified based on the likelihood of a security incident occurring due to the open access permissions of the information system. The severity of potential incidents was evaluated by considering their impact on daily operational needs.

# **Remediation Strategy**

To secure the database server, it is recommended to implement robust authentication, authorization, and auditing mechanisms to ensure only authorized users can access it. This includes enforcing strong password policies, utilizing role-based access controls, and implementing multi-factor authentication to restrict user privileges appropriately. Encrypt data in transit using TLS instead of SSL, and use IP allow-listing for corporate offices to prevent unauthorized internet users from connecting to the database. Additionally, implementing a load balancer and block communication through outdated or unused ports, protocols, and applications can help from potential issues to occur in the future.