**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**

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

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |
| *System administrator* | *Craft counterfeit certificates* | *2* | *3* | *6* |

# **Approach**

The risks selected considered the data storage and management procedures of the business. The potential threat sources were weighed up between how likely they were to occur and how severe an impact it would have on the company. These weights also take into consideration the open access permissions of the database.

**Remediation Strategy**

The implementation of authentication, authorization and auditing mechanisms ensure that only authorized users can access the database. This includes strong password standards, role-based access controls and Multifactor Authentication (MFA) to limit user privileges. When the data is considered “in motion”, TLS standards are more effective than SSL. IP whitelisting to corporate offices prevents random users from connecting to the database outside the network.