**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/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) 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 Database server is a centralized computer that has constant access to customer data that is regularly quarried and/or requested to help find future customers. It houses stored Customer data as well as campaign and analytical data which are company assets used to help the company track and personalize marketing efforts that could be taken advantage of by unknown threats.***

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Employee* | *Disrupt mission-critical operations* | *2* | *3* | *6* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

# Approach

Risks considered are the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

1. **Being that the data is being kept in one centralized location that contains lots of company assets and customers personal data it would be an ideal target for an outside hacker to target that would gain them lots of assets and potentially do lots of damage to the company in the process**
2. **Employees are sometimes the biggest threats to an organization as they can unknowingly be putting the company at risk by either not having a good enough password, clicking on links they shouldn’t, or if they are an unhappy employee they could leak data on purpose while being granted access to company assets.**
3. **If not configured properly customers could potentially have access to sections of the company they shouldn’t such as having access to company campaign records.**

# Remediation Strategy

**Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database. Principle of Least privilege should be implemented, so that employees only have access to the amount of data and information required to their job and nothing more, making it much harder for information to be leaked out either on purpose or by accident.**