**Vulnerability Assessment Report**

**1st January 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 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

The database is quite important and valuable for the business due to the fact that it's a small business based on e-commerce. The company stores information on a remote database server, since many of the employees work remotely. It’s important to keep the data secure for maintaining safe all of the customers and vendors’ private info. The business is based on e-commerce so if the server went down, it would impact the business horribly. Stores and manages large amounts of data, it stores customer, campaign and analytic data, it is critical to secure the system because of its regular use for marketing operations.

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Hacker/employee* | *Conduct Denial of Service (DoS) attacks* | *2* | *3* | *6* |
| *Hacker/employee* | *Perform reconnaissance and surveillance of organization* | *2* | *2* | *4* |
| *Employee* | *Alter/Delete critical information* | *2* | *3* | *6* |

# Approach

Talking about the threats above, the fact that the server is public makes it a very risky situation for the business. We spotted three potential risks that in a future will happen, for example a denial of service attack could flood the server and completely shut down the entire server. Any employee could alter or delete any kind of critical information that would cause the daily activity of the business to stop. Some hacker or employee could perform reconnaissance and surveillance of the organization due to the public constitution of the server. Any competitor could get or obtain sensitive information about the business via exfiltration. The threats that were mentioned first are the ones that have the most risk to happen.

# Remediation Strategy

So, to remediate or mitigate these threats we will have to make the server more private that it already is. For this, we are going to add some security controls like the principle of least privilege: each employee will have the access based on their current role, not further permissions, just the ones that they already need. Secondly, we are going to implement multi-factor authentication (MFA) to limit user privileges, in that way we assure that the authentication process is quite secure. Thirdly, we think it’s better if we use separation of duties, in that way if some employee's computer is compromised, it wouldn’t affect the others in the server. Lastly, we are going to implement public key infrastructure to address the exfiltration of sensitive information and IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.