**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 contains sensitive information relating to customers and possible future customers. Securing the data on the server is essential in making sure the information used by the sales team is accurate. It will also help with compliance issues, as there are many regulations surrounding the security of secure personally identifiable information. If the server were disabled, no sales would be able to occur.

# **Risk Assessment**

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Perform reconnaissance and surveillance of*  *organization* | *3* | *2* | *6* |
| *Malicious Software* | *Install persistent and targeted network sniffers*  *on organizational information systems.* | *3* | *2* | *6* |
| *Hacker* | *Disrupt mission-critical operations.* | *3* | *3* | *9* |

# **Approach**

The threat sources listed are likely to appear and would not have any trouble in conducting the threat events listed. Because the server is open to the public, competitors are able to survey the traffic across a network. The information in the server would be open to them to steal possible business or disrupt current operations. Similarly, hackers and malicious software could achieve the same things but for different reasons. The severity of these events should not be overlooked, as any one of them could disrupt business operations severely. Damage to data may be fixed, but the damage to the brand reputation may be irreversible.

# **Remediation Strategy**

It seems that there are no current operations in place to ensure that the data on the server is protected. There are no authorization or authentication safeties in place to ensure that threat actors can not perform their attacks. Some recommendations are as follows:

* Create user roles for employees
* Make the server private, contained in the internal network
* Conduct authorization audits to ensure least privilege is being practiced
* Use MFA to ensure that users are authentic

Using these strategies should help increase the security posture of the organization as a whole and fix the current glaring issue with the server.