**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" \l "heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

The database server is used frequently by employees located all over the world to find potential customers, so it is an important asset. The data on the server is PII which is protected by law and must be secure from unauthorized access. If this server was disabled this would negatively affect business operations. This database is open to the public which represents a security problem.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Outside Hacker* | *Accessing PII for malicious purposes* | *3* | *3* | *9* |
| *Competitor* | *Accessing PII for business purposes* | *3* | *3* | *9* |
| *Employee* | *Accessing PII for malicious purposes* | *1* | *3* | *3* |

# **Approach**

I selected these risks because they seem to be the most likely sources of misuse of PII. I estimated that the likelihood of an outside hacker or competitor accessing and using the PII in the database to be high because there is nothing stopping them from doing so and there would be a financial benefit. I think it is possible that an employee could also use this information for malicious purposes, but employees should be more trustworthy than people outside the company. It is possible that there are other risks I have not considered due to the database being publicly accessible by anyone.

**Remediation Strategy**

An Identity and Access Management system should be implemented so that only employees can access the database. This should include strong passwords an multi-factor authentication. Furthermore, only employees that need to access the database should be allowed to access it, based on their role in the company. The data in the database contains PII, so it should be encrypted with a strong encryption standard to ensure compliance with data protection laws, and prevent the data from being leaked.