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 is used to guide the risk analysis of the information system.

Purpose

The database server is a crucial part of the business as it enables the employees from any location on the globe to find the potential customers by querying or requesting data from the server.

The server is currently made public which is a large security risk as it means anyone can access the server and the data stored on it. Making it secure will minimize the risk of any threat actors being able to access the data or use the server to connect to internal servers of the company. Also, If the data stored on the server are PII or SPII it would be recommended to secure the server by using proper authentication and authorisation techniques and by encrypting the data stored on the servers. That way we ensure that the company would comply with required legislations around the world. This would help to avoid potential breaking of the law but also would avoid causing potential damage to the company itself in case the personal data was to be leaked or stolen by the threat actor. This could also involve confidential company data as well.

If the server were to be disabled for any reason which might as well be due to malicious attack by an external threat actor it would make the company unable to function and do the business as usual. The employees would not be able to access the data which would make it impossible or difficult for them to find new customers.

-

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*DOS attack by overwhelming the servers with large amount of requests*	*3*	*3*	*9*
Unauthorized users	*Due to lack of access controls, an unauthorized person could access sensitive data.*	*2*	*2*	*4*
Malicious software	*An threat actor could install an malicious software on the server*	*2*	*3*	*6*

Approach and possible remediation strategies.

I have chosen the three specific threat sources/events above as I believe they would represent significant risks to the business.

The Hacker could gain access to the servers very easily considering they are open servers assuming there are no IAM controls in place etc. For example DOS attack would make the servers inaccessible to the employees trying to access the data they need to do their jobs as the server would stop responding due to being busy trying to deal with hundreds of thousands of requests attacking the servers, initiated by a threat actor.

Unauthorized users would enable anyone to potentially gain access to any data stored on the servers. The data stored on the servers might be sensitive data or not all data is necessary to do the job of the individual employees. The proper IAM controls should be implemented, with help of MFA or SSO as well. The least privilege principle should be implemented as well making sure that only data required for each employee to do their job is accessible to them. The separation of duty should be also implemented making sure that the tasks are split to different employees minimizing the risks of employees abusing their role.

The Malicious software could cause a lot of issues completely disabling the servers and potential even spreading further in other devices or into other parts of the internal company network systems. Strong access controls, network segmentation, firewalls etc.

In general the company should look into cybersecurity strategy such as defense in depth which will involve layering multiple security measures through an IT infrastructure to provide redundancy and enhance overall security.