**Vulnerability Assessment Report**

**1st January 20XX**

# **Scenario**

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.

# **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**

This database server is an extremely critical piece of the daily operations of this business. If the server were to go down, all business operations would grind to a halt. That is why the highest priorities should be to keep the server secure and ultimately keep it up and running so that employees can continue to make use of it.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Hacker* | *Encryption and ransom of critical data* | *3* | *3* | *9* |
| *Employee* | *Alter/delete critical data* | *2* | *3* | *6* |

# **Approach**

Given the relatively open-access nature of the database server and how frequently the data on it is used, I chose to focus on risks that pertained to the manipulation of that data. Those risks scored very high, and that is because of the very high importance I imagine this company places on the server. It would seem that day to day operations would be severely hampered by any outage of the server.

# **Remediation Strategy**

Assuming they are not already in place, basic policy level security measures would be in order. These would include the requirement of strong passwords, multi-factor authentication, and the principle of least privilege. On the technical side, the server uses a mix of the older and less secure SSL communication protocol and the newer TLS protocol. The entire server should be using TLS in order to ensure that it is making use of the most modern security features. On top of all that, constant monitoring of the network, both by humans and IDS/IPS systems will be necessary.