Scenario Description (FYI)

I am working in an E-commerce company. The database of the company is a remote one, and the staff query to use the database from all around the world remotely very often. The database is open to public since the company is launched 3 years ago. I recognized that opening database to public leads to serious issues.

Vulnerability Assessment Report

17th 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 is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

The database is used since the launch of our company for staff all over the world to remotely query data from it to find potential customer. It saved most of the company data and is a connection point of staff of all branches. The server is connected with other server in the network, but it is open to the public, which is a serious backdoor for malicious actors. The global operation of our company will be affected, and potential economic consequences will occurred due to data leakage if the database is disabled.

This vulnerability assessment will target on the access control in this server, to secure the data of also the whole network by identifying vulnerabilities, analyzing vulnerabilities, prepare defense and incident response of threat and for further defense system testing.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	3	3	9
Hacker	Conduct Denial of Service (DoS) attacks	3	3	9
Storage	Disrupt mission-critical operations	2	3	6

Approach

Considering the major vulnerabilities of the server - opening to public, 128 GB storage and one server for employees all over the world. I select the top 3 risks by evaluating the source of human, technological and environmental dimension to avoid overlapping and extend the protection of the future security posture.

The limitations of the assessment is the threats mentioned might not covered all the threat related to vulnerabilities. And the remediation might be costly and is a long term progress.

Remediation Strategy

1. Clear access distribution: Revoke access completely from outsiders and prioritize the access of internal staff to improve separation of duties and principle of least privilege.
2. Security measures on the perimeter level should be enhanced, including setting up firewall, end-point protection, allowing MFA in the log in system.
3. Database distribution: as 128GB is not enough for future usage, and to separate data by regions for efficient data enquiry, multiple database providing service regionally, such as asia-pacific region or american region, should be set up.
4. Back up server: there should be back-up server which its access is set to be restricted in case the main server is disabled.