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.

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.

Purpose

This database server acts as the main repository for the company's e-commerce information. If this database was compromised the data could be altered, deleted, exfiltrated by competitors or threat actors or used in a ransomware attack on the company. Any of these scenarios would be highly detrimental to business operations, company reputation and morale, and bring the company into the notice of multiple regulatory bodies such as the SEC.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information*	*3*	*3*	*9*
Suppliers	*Obtain sensitive information*	*1*	*2*	*2*
Employees	*Disruption of current business practices in a number of ways*	*1*	*3*	*3*

Customers	*Alter/Delete critical information*	*1*	*2*	*2*
Outside Threat Groups (Hackers)	*Disruption of current business practices in a number of ways*	*2*	*3*	*6*
Technological Failures	*Hardware failure requiring back-up systems online*	*2*	*2*	*4*

Approach

The threats in the Risk Assessment were chosen for being the ones most usually associated with a situation similar to the provided scenario. Like any assessment this can only serve as general guidelines for possible threats and attempting to outline the most likely ones. In real world situations the threat environment is deep and the reasons for such attacks are greatly varied, though many often result in the same business disruptions.

Remediation Strategy

To better secure the system we have a number of recommendations.

- *Implement individual account authentication procedures such as username/password for each authorized user, whether internal or external to the company*
- *Enforce role-based access in order to control data access according to the needs of each user account*
- *Create and implement procedures to ensure all data is backed up to other servers and media on a timely and consistent basis*
- *Implement data access logging for forensics investigations*