Vulnerability Assessment Report

15th Feb., 2026

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.

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 2026 to August 2026. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is valuable to the company as it allows our personnel to access much needed data about potential customers and therefore is a driving source of expanding the organization's customer base and overall profits. Furthermore, the database holds PII information and, depending on where certain employees and potential customers are located, the database having unauthorized access can lead to a violation GDPR compliance and non-compliance of NIST CSF which is a driving framework for hosting a secure system. If a threat actor were to gain access to this database and use data unethically, change data, or take the database offline it could critically impact business operations and open the organization up to potential fines, reputation loss, and legal implications.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Standard user	*User unknowingly or maliciously deletes or changes data*	*2*	*3*	*6*
Hacker	*Obtain, change, or delete data maliciously. Can use it to gain access to a different network segment*	*1*	*3*	*3*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. The human factors were the prime focus as the highlight of the assignment was that the database was open to the public.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing via firewall to corporate offices to prevent random users from the internet from connecting to the database.