Vulnerability Assessment Report

Scenario

An e-commerce 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, I recognize that keeping the database server open to the public is a serious vulnerability.

Here I have created a written report that explains how the vulnerable server is a risk to business operations and how it can be better 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 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server computer system which holds and manages data in reference to the customers and potential customers of the company. The server holds data which helps to analyze information based on individuals which can help to personalize marketing strategies and goals for the company. This is a server which is regularly used and if data falls into the wrong hands, it would disrupt the day-to-day activities of the business as well as threaten the reputation of the company

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Threat actor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt day to day operations for their own gain*	*2*	*3*	*6*
Customer	*Alter information*	*2*	*3*	*6*

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.

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 to corporate offices to prevent random users from the internet from connecting to the database.