

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](#) is used to guide the risk analysis of the information system.

Purpose

Consider the following questions to help you write:

This database server is valuable to the business as it contains all the important information that runs the business. These include customers' information, campaign, and analytic data. It is important for the business to secure the data on the server in case of an infiltration or exfiltration, causing a massive data leak that can be very damaging. It is very important to keep this database secured from potential threats and vulnerabilities.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
<i>Hacker</i>	<i>Obtain sensitive information via exfiltration</i>	3	3	9
<i>Employees</i>	<i>Disrupt mission-critical operations</i>	2	3	6
<i>Customers</i>	<i>Alter/Delete critical information</i>	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.

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.