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. A vulnerability assessment of the situation can help you communicate the potential risks with decision makers at the company. You must create a written report that clearly 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

The database server is a big computer that holds and looks after a lot of data. It keeps info like customer details, campaign stuff, and analytics, which can be checked later to see how things are going and to make marketing more personal. It's super important to keep it safe since it's used a lot for marketing work.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacktivist	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*After/delete data*	*1*	*4*	*5*
Power Outages	*Unable to have the systems online*	*3*	*7*	*10*

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. A hacktivist poses a risk by breaking into systems and stealing sensitive information through exfiltration, meaning they secretly transfer data out. Once they have this information, they can leak it publicly or use it to harm the company's reputation or operations. A customer can be a risk if they can change or delete important data, either accidentally or intentionally, disrupting records or business processes. This could lead to data loss, errors, and costly recovery efforts if access isn't properly controlled. A power outage is a risk because it takes systems offline, stopping access to important data and disrupting business operations. It can also lead to data loss or leave the company vulnerable to security threats if backup systems aren't in place.

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. A good strategy for handling power outages is to have backup power sources, like generators or uninterruptible power supplies (UPS), to keep essential systems running. Additionally, regularly backing up data and having a disaster recovery plan in place ensures critical information and operations can be restored quickly once power returns.