Vulnerability Assessment Report

29th January 2025

System Description

This assessment focuses on a publicly accessible remote database server containing e-commerce customer data. Employees query this server globally for potential customers. The system's attack surface includes its open internet port, potential DBMS vulnerabilities, weak access controls, and unencrypted data transmission..

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 critical asset for the business as it stores and manages large amounts of data, including customer, campaign, and analytic data. This data is essential for tracking performance and personalizing marketing efforts, which directly impacts the business's ability to attract and retain customers.
- It is important to secure the data on the server due to its regular use for marketing operations. A security breach could lead to the loss of sensitive customer data, financial losses, and a decline in customer trust. Additionally, if the server were disabled, the business would not be able to effectively track performance and personalize marketing efforts, which could lead to a decline in sales and revenue.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission critical operations*	*3*	*3*	*6*
Customer	*Alter/Delete critical information*	*3*	*3*	*3*

Approach

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

Remediation Strategy

The remediation strategy should focus on:

- Implementing authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server.
- Encrypting 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.