Vulnerability Assessment Report

3rd June 2024

In this project I conducted a scenario vulnerability assessment for a small business.

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 April 2024 to June 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. It is critical to secure the system because of its regular use for marketing operations. Data should be secured to protect the confidentiality, integrity and availability of consumer data. If data is not secured and the organization is in risk of not being in compliance with information privacy standards which could lead to fines. If the server is to fail the organization could face the exposure of sensitive consumer information.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	*1*	*3*	*3*

Hacker	Gain PII from database server	2	*3*	*6*
Advanced Persistent Threat	Threat actor has access to information for an extended period of time	3	*3*	*9*

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.

Competitors have access to obtain sensitive information of customers via exfiltration and could take away business opportunities. Hackers could gain access to personally identifiable information (PII) provided in the database server to commit identity theft, which would lead to a damage of the company's reputation. Advanced Persistent Threats could also occur being that threat actors have public access to customer data for an extended period of time.

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.