Vulnerability Assessment Report

10th April 2025

System Description

I work with an e-commerce company, the company system is used to support remote operations and marketing efforts. It is a centralized server that stores sensitive business data, including potential customers information, it is accessible over the internet and has been open to the public since the company launched three years ago. Staff members access the database from various global locations. They regularly query the server to retrieve customer data for lead generation and sales campaigns. Currently, the server has no access restrictions or authentication mechanisms in place, this means that anyone with the server's IP or URL can access the database without validation, making it highly vulnerable to unauthorized access.

Scope

This assessment focuses on evaluating the security risks of the company's publicly accessible remote database server. It includes identifying vulnerabilities in access controls, analyzing employee access methods, and determining potential threats to sensitive business data. The goal is to recommend steps to secure the server and protect company operations.

Purpose

The purpose of this assessment, in accordance with *NIST Special Publication 800-30 Revision 1*, is to conduct a risk-based evaluation of the publicly accessible remote database server used by the e-commerce company. This assessment aims to:

- Identify threats and vulnerabilities affecting the system;
- Determine the likelihood of exploitation;
- Analyze the potential impact on business operations, data confidentiality, integrity, and availability;
- Support risk-informed decision-making by providing recommendations for risk mitigation and improved security posture.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitors	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*
External attacker	*Unauthorized access to public database*	*3*	*3*	*9*
Malicious insider	*Data exfiltration or unauthorized queries*	*2*	*3*	*6*
Advanced Persistent threat (APT)	*Perform reconnaissance and surveillance of organization*	*2*	*2*	*4*
Malicious Software	*Install persistent and targeted network sniffers on organizational information systems.*	*3*	*3*	*9*
Ransomware group	*Deployment of malware via open server access*	*1*	*3*	*3*

Approach

- **Competitors**: has a medium risk score and the impact on the business is that there will be loss of strategic advantage and revenue loss.
- **External Attackers**: it has a high risk score and the impact will be a data breach, financial loss, reputational damage.
- **Malicious Insider**: It has a medium risk score, and this impact can be data tempering, difficulty in detecting the attacker and operational risk.
- **Malicious Software**: It has a high risk score, and the impact to the business can be systems being disrupted, loss of data and breach of customers trust.

Remediation Strategy

- Implement multi-factor authentication and role-based access controls to restrict database access to authorized users only.
- Deploy a firewall and intrusion detection system to monitor and block unauthorized access attempts.
- Regularly patch the database software and provide ongoing cybersecurity training to employees to reduce vulnerabilities and insider risks.