Vulnerability Assessment Report

4/23/2025

System Description

The system under assessment is a remote access database server that supports the core operations of a global e-commerce business. The server stores valuable business and customer data and is queried regularly by employees working remotely from around the world. It has been publicly accessible via the internet since the company's launch. This exposure increases its vulnerability to unauthorized access, data exfiltration, and denial of service attacks. The system includes the database infrastructure, network configuration, remote access methods, and related authentication mechanisms used to support employee queries.

Scope

This assessment focuses on the confidentiality, integrity, and availability of data stored and transmitted through the publicly accessible database server. It covers remote access vulnerabilities, risks related to external actors such as hackers, competitors, hacktivists, and internal misconfigurations that may expose sensitive business data. The assessment excludes physical security measures, other company systems not related to this database, and endpoint devices used by employees. The primary objective is to identify cybersecurity risks and propose mitigation strategies for the exposed server infrastructure.

Purpose

The purpose of this vulnerability assessment is to evaluate the risks associated with a publicly accessible database server used by the e commerce company. The server is critical to the business because it stores customer data and supports remote access for employees conducting customer research. Securing the data is essential to maintain customer trust, ensure data integrity, and meet legal and regulatory obligations. If the server is compromised or disabled, business operations could be disrupted, leading to data loss, reputational damage, and financial penalties.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Competitor	*Perform reconnaissance and surveillance*	*2*	*2*	*4*
Hacktivist	*Conduct Denial of Service (Dos) attacks*	*3*	*2*	*6*

It is highly likely for a hacker to exploit a publicly available server to steal customer or internal data. This would in turn pose a catastrophic threat to the business. For Competitors, may passively scan for vulnerabilities to gain strategic advantage. A Hacktivist is likely to launch Dos attacks to make a statement or disrupt operations, which could significantly slow or halt the service.

Approach

I used a qualitative approach based on NIST SP 800-30 Rev. 1. I selected threats that are both relevant to publicly exposed infrastructure and realistic based on current threat intelligence. For example, hackers and hacktivists are common external threats to remote access systems. I estimated likelihood and severity using a scale of 1 to 3 based on how accessible the system is, the sensitivity of the data, and the potential for business disruption. While this assessment does not include physical or internal system risks, it provides a focused analysis of high-impact externally driven risks.

Remediation Strategy

To mitigate the risks identified, the business should implement multiple security controls. First, remove public access to the database and restrict access via a VPN with multi-factor authentication (MFA). Enforce the principle of least privilege to ensure employees only access the data they need. Implement defense in depth using firewalls, intrusion detection systems, and regular audits. Then encrypt all data in transit and at rest, and establish logging and monitoring protocols to detect unusual activity. These measures would significantly reduce the likelihood and impact of unauthorized access and system disruption.