Vulnerability Assessment Report

System Description

Our company runs on a distributed remote-first setup. A cloud-hosted database server holds customer-related data and supports business development operations. Staff from all over the world access it daily. But here's the issue—it’s been open to the public since the business launched. That’s three whole years of unrestricted access.

Scope

This report strictly looks at risks around the data stored on that database—so, things like confidentiality, availability, and integrity. We're not diving into hardware or other external IT systems. The spotlight is solely on this server and the data it holds.

Purpose

As the newly onboarded cybersecurity analyst, I spotted an urgent problem: the server’s public exposure. This assessment is meant to lay bare the risks, paint a picture of what could go wrong, and offer up practical solutions. It's about protecting the business and its data, plain and simple.

Threat Identification

We’ve identified a few pressing threats:

- Hackers scanning for open services—this server is low-hanging fruit
- Insiders with too much freedom—could misuse or leak data
- Automated bots that probe servers daily, non-stop
- More advanced threat actors going after customer databases for profit

Vulnerability Identification

Here’s what’s making us vulnerable:

- Server is publicly accessible—no access restrictions at all
- No login barrier or encryption (yep, it's that open)
- Not segmented from other systems—everything talks to everything
- Lack of monitoring or alerts when something goes wrong

Risk Assessment

Risk	Likelihood	Impact
Unauthorized Data Access	High	Severe (data leak, legal trouble)
Data Integrity Compromise	Medium	Moderate (loss of trust, system errors)
Service Disruption (DoS)	Medium-High	High (downtime, lost revenue)

Recommended Controls

We’ve got a few solutions to help fix the open door:

- Restrict access using firewalls or VPNs—shut the front door
- Enable multi-factor authentication and proper user roles
- Encrypt data in transit and at rest (TLS/SSL, AES)
- Set up monitoring tools to catch suspicious behavior early
- Regularly audit the server and patch any known weaknesses

Report written and compiled by Abubakari-Sadique Hamidu
For portfolio and educational purposes only.