Scenario

You are a newly hired cybersecurity analyst at a mid-sized e-commerce company that relies heavily on digital marketing for revenue.

The company maintains a **cloud-hosted PostgreSQL database** containing over **three years' worth of customer prospect data**, including **personally identifiable information (PII)** such as names, emails, phone numbers, and partial payment data.

This database plays a crucial role in the company's operations: it supports **targeted marketing campaigns**, which drive approximately **35% of monthly revenue**. The database is **queried daily by around 120 remote employees** from around the globe, who use a combination of **web-based dashboards and direct SQL clients** to access the information.

Since the company's launch, however, the **database has remained publicly accessible over the Internet**. There is **no authentication**, **no network filtering**, and **default roles** are still active. In fact, **port 5432 is openly reachable**, exposing the system to anyone scanning for open PostgreSQL services.

As a cybersecurity professional, you immediately recognize that leaving this database exposed represents a **significant security vulnerability**. You are tasked with conducting a **vulnerability assessment** following **NIST SP 800-30 Rev. 1 guidelines**, and creating a **written report** to help decision makers understand:

- The **business and technical risks** posed by the current configuration,
- The **impact** of potential threat events,
- And how the situation can be remediated through appropriate controls.