Vulnerability Assessment Report

Executive Summary

This vulnerability assessment, conducted in alignment with NIST SP 800-30 Rev. 1, evaluates a critical exposure affecting the company's cloud-hosted PostgreSQL database, which has been publicly accessible without authentication since launch.

The database contains over 1.4 million records of personally identifiable information (PII) including names, emails, phone numbers, and partial payment data. It is queried daily by approximately 120 remote employees through a combination of web applications and direct SQL clients, supporting targeted marketing campaigns that generate roughly 35% of the company's monthly revenue.

Key Findings:

- **Exposure Risk**: The database is accessible on the open Internet via port 5432, with default credentials and no firewall restrictions, making it highly vulnerable to external exploitation.

- **Top Threat Scenario:** A remote attacker could easily exfiltrate full customer datasets, resulting in severe GDPR violations, brand damage, and regulatory fines. This event was scored with the highest risk rating (9 – High)using NIST's Likelihood × Impact model.

- **Other Risks**: Moderate risks were identified in insider-triggered data deletions and DoS (Denial-of-Service) attacks that could **disrupt business-critical operations** during peak marketing cycles.

Business Impact:

- A successful breach could lead to an estimated €2.4 million in regulatory penalties, incident response costs, and lost business, greatly surpassing the cost of remediation.

- Continuation of the current setup **violates data protection best practices**, increases legal liabilities, and undermines customer trust.

Immediate Recommendations:

1. Restrict Public Access (P1): Place the database behind a VPN or zero-trust proxy, enforce strict IP whitelisting, and close public ports.

2. Implement Access Controls (P2): Enable RBAC, disable default accounts, and introduce multi-factor authentication.

3. Encrypt and Monitor (P3–P4): Enforce encryption in transit and at rest, and implement SIEM-based centralized logging with ECC (Error Correcting Code) integrity.

4. Strengthen Operational Security (P5–P8): Regular backups, DoS mitigation, insider-threat training, and strict patching SLAs.

Risk Reduction:

Implementing the top four controls (P1–P4) reduces the likelihood of data exfiltration from High (3) to Low (1) and lowers the overall risk score from 9 to 3, shifting it into the low-to-moderate category.

Strategic Recommendation:

- **Immediate Action**: Prioritize implementation of the first four risk mitigations within **10 business days**.
- **Budget Alignment**: The full control set is estimated at **€80,000**, significantly lower than the potential cost of a breach.
- **Ongoing Governance**: Embed NIST-style assessments into the company's quarterly risk review and change management processes.

Conclusion:

The company must act decisively to close this critical vulnerability. The cost of inaction is high, while remediation is straightforward, measurable, and fully aligned with industry standards.

Assessment

1 Purpose & Scope

The objective of this assessment is to demonstrate—using the NIST SP 800-30 risk-assessment process—why the company's customer-prospecting database, left open to the public for three years, poses an unacceptable risk to confidentiality, integrity, and availability, and to recommend a prioritized set of controls.

NIST SP 800-30 provides the systematic steps to **identify threats and vulnerabilities, determine likelihood and impact, calculate risk, and support informed risk-response decisions.**

2 System Characterization

Item	Description
Asset	Cloud-hosted PostgreSQL cluster containing 3 years of prospect and limited customer PII (names, e-mails, phone numbers, partial payment data).
Access pattern	Queried daily by ~120 remote employees via a web UI and direct SQL clients.
Current exposure	No network filtering, no authentication, port 5432 reachable on the public Internet, default database roles.
Business role	Drives targeted marketing campaigns that generate ~35 % of monthly revenue.

3 Threat Sources & Threat Events

Threat source (examples)	Relevant threat events for an open DB server
External attackers – Hackers, APT (Advanced Persistent Threat) groups, competitors	Reconnaissance & vulnerability scanning • Credential-stuffing or brute-force login • DoS (Denial-of-Service) flood • "Man-in-the-Middle" packet capture
Privileged insiders – System administrators, DevOps contractors	Unauthorized data export • Stealth schema changes to hide fraud

Standard users – Sales staff with legitimate access	Accidental mass deletion or update
Environmental / service failures – Cloud node outage, power loss	Abrupt service interruption leading to inconsistent data

NIST SP 800-30 defines these actors and actions exactly as *threat sources* and *threat events* that can "negatively impact an organization's information systems" .

4 Likelihood Determination

NIST recommends qualitative scoring (High = 3, Moderate = 2, Low = 1) based on intent, capability, precedent, and controls in place .

Representative threat event	**Factors**	**Likelihood score**
External attacker exfiltrates full table via unauthenticated connection	• Asset is Internet-facing • No credential barrier • Similar breaches widely reported	3 (High)
Insider mass-deletes prospect records	• Privileged logons share same password • No change control	2 (Moderate)
DoS floods TCP 5432, disrupting queries	• No rate limiting or WAF (Web Application Firewall) • Commodity tools automate attack	2 (Moderate)

5 Impact (Severity) Determination

Using NIST's 1-to-3 scale:

Consequence area	**Impact rationale**	**Severity score**
Confidentiality	Loss exposes prospect records → potential GDPR fines and brand damage	3 (High)
Integrity	Unnoticed data alteration corrupts lead-ranking algorithm → revenue loss	2 (Moderate)
Availability	Hour-long outage during campaign launch → lost sales, SLA penalties	2 (Moderate)

6 Risk Calculation & Prioritization

NIST: Risk = Likelihood × Impact

Threat event	Likelihood	Impact	Risk score	Risk level
External data exfiltration	3	3	9	High
Insider deletion	2	2	4	Moderate
External DoS	2	2	4	Moderate

Scores 6-9 = High, 3-4 = Moderate, 1-2 = Low. Exfiltration is clearly the top risk.

7 Recommended Risk Responses

Priority	Control or activity	Mapped NIST 800-53 Controls
P1	**Remove public network exposure**: place DB behind VPN or zero-trust proxy; restrict inbound CIDR to corporate IP ranges	- **AC-4**: Information Flow Enforcement - **SC-7**: Boundary Protection
P2	**Enforce strong authentication & RBAC (Role-Based Access Control)**; disable default “postgres” user; individual least-privilege roles	- **AC-2**: Account Management - **AC-6**: Least Privilege - **IA-2**: Identification and Authentication
P3	**Encrypt data in transit and at rest** (TLS with modern cipher suites; AES-256 for storage)	- **SC-12**: Cryptographic Key Establishment and Management - **SC-13**: Cryptographic Protection - **SC-28**: Protection of Information at Rest - **SC-12(2)**: Symmetric Keys - **SC-12(3)**: Asymmetric Keys
P4	**Continuous monitoring & logging**: central SIEM ingest of query logs; alert on anomalies; implement ECC (Error Correcting Code) storage for logs to prevent tampering	- **AU-2**: Event Logging - **AU-6**: Audit Record Review, Analysis, and Reporting - **SI-4**: System Monitoring - **AU-9**: Protection of Audit Information
P5	**Regular backup & integrity checks**; quarterly recovery-time objective (RTO) tests	- **CP-9**: System Backup - **SI-7**: Software, Firmware, and Information Integrity

P6	**Web Application Firewall / rate-limiter** in front of application layer; automated blocking of DoS patterns	- **SC-5**: Denial of Service Protection - **SC-7(11)**: Restrict Incoming Communications Traffic
P7	Security awareness & insider-threat program for remote staff	- **AT-2**: Literacy Training and Awareness - **PM-12**: Insider Threat Program
P8	**Patch management cadence**: monthly engine and OS updates, zero-day emergency SLA ≤ 48 h	- **SI-2**: Flaw Remediation - **CM-2**: Baseline Configuration - **CM-3**: Configuration Change Control

8 Residual Risk & Continuous Assessment

After implementing P1–P4, the exfiltration scenario likelihood drops to **1 (Low)** and risk to **3 (Low-Moderate)**.

NIST stresses that risk assessment is a **repeatable, documented, and integrated process**; re-assess after any major system change or at least annually to ensure controls remain effective.