Vulnerability Assessment Report

System Description

The database server is equipped with a state-of-the-art CPU and has a memory capacity of 128GB. Operating on the latest Linux version, it houses a MySQL database management system. Network-wise, the server operates using IPv4 addressing and maintains connections with several other servers in the company's infrastructure. To secure data transfers, SSL/TLS encryption is in place, which provides a foundational layer of security against data interception during transmission.

Scope

For this vulnerability assessment, the primary focus is on the access controls currently implemented on the server. The assessment timeline spans three months, specifically from June to August 2023. The process and methodologies employed are aligned with the guidelines set forth by NIST SP 800-30 Rev. 1, ensuring a standardized approach to risk analysis for our information systems.

Purpose

Our e-commerce company, leveraging a globally distributed workforce, relies heavily on the database server to enable employees to pinpoint potential customers and craft effective sales initiatives. With the digital landscape being at the forefront of our operations, securing server data is imperative, not just for preserving customer confidentiality and business insights, but also to remain compliant with international data protection laws. A breach or server downtime would place the business in peril, opening possibilities for legal repercussions, diminishing customer trust, and considerable financial loss.

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk
Hacker	Conduct Denial of Service (DoS) attacks.	3	3	9
Competitor	Obtain sensitive customer information via exfiltration.	3	3	9
Outsider	Perform reconnaissance and surveillance of organization.	2	2	4

Approach

Considering the company's open server configuration, we pinpointed these specific threat sources and events. The open nature of our server makes it a prime target for hackers aiming to disrupt our services. Competitors, spotting an opportunity in our exposed stance, might attempt

to drain sensitive customer data. Additionally, outsiders, be it curious individuals or novice hackers, could exploit the server's openness to reconnoiter our database, potentially leading to unnoticed breaches.

Remediation Strategy

Addressing the heightened risk posed by the server's public accessibility, the following immediate actions are advised:

- Restrict Server Access – The database server should promptly be shielded from public access. Only recognized IP addresses, such as those affiliated with our employees or vetted partners, should gain access.
- Implement VPN – Given the global dispersion of our workforce, initiating a secure VPN is crucial. This would grant employees secure database access without subjecting it to external threats.
- Enforce Multi-Factor Authentication (MFA) – Mandate MFA for all users, particularly those with elevated privileges.
- Adopt Authentication, Authorization, Accounting (AAA) Framework – Incorporate a robust AAA mechanism to bolster access controls, ensuring meticulous vetting of users, assignment of precise permissions, and rigorous action auditing.
- Conduct Routine Security Audits – Considering the server's prior public exposure, periodic security audits are vital. Such audits will uncover any residual vulnerabilities and check for potential data integrity issues.

By integrating these remediation steps posthaste, the company can drastically cut down the risk of cyber breaches, safeguarding the integrity and consistent availability of the pivotal database server.