Vulnerability Assessment Report

1st January 2025

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 2025 to August 2025. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The databased server is very valuable to the business as it is a centralized computer system that stores and manages large amounts of data, and it interacts with other servers on the network, many of them are from employees that work remotely from locations all around the world. It is critical for the business to secure the server because it is regularly used for the company's marketing and sales operations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations.*	*2*	*3*	*6*
Customer	*Alter/Delete critical information.*	*1*	*3*	*3*

Approach

The measured risks took into account the business's data storage and management practices. Potential threat sources and events were identified based on the likelihood of a security incident due to the system's open access permissions. The severity of possible incidents was assessed in relation to their impact on daily operations.

Remediation Strategy

To enhance database security, implementing robust authentication, authorization, and auditing mechanisms is essential to ensure that only authorized users can access the database server. Key measures include:

- **Strong Authentication Controls:** Enforce the use of strong passwords, role-based access controls (RBAC), and multi-factor authentication (MFA) to minimize unauthorized access.
- **Comprehensive Authorization Policies:** Restrict user privileges based on the principle of least privilege (PoLP), ensuring that users can only access the data necessary for their roles.
- **Auditing and Monitoring:** Implement continuous logging and monitoring of database access and user activity to detect and respond to suspicious behavior in real time.
- **Data Encryption:** Encrypt data in transit using TLS instead of SSL to protect sensitive information from interception. Additionally, encrypt data at rest to safeguard stored information.
- **Network Security Controls:** Implement IP allow-listing to restrict database access to corporate offices, preventing unauthorized connections from the internet. Use firewalls and VPNs to secure remote access.
- **Regular Security Assessments:** Conduct periodic security audits, vulnerability assessments, and penetration testing to identify and remediate potential risks proactively.
- **Patch Management:** Regularly update database software, operating systems, and security patches to mitigate vulnerabilities.
- **Incident Response Plan:** Develop and test an incident response plan to ensure a swift and effective response to security breaches.

By integrating these remediation strategies, organizations can significantly reduce the risk of unauthorized database access and data breaches.