Vulnerability Assessment Report

Date: January 20XX

System Description

The system is a remote database server utilized by the company for storing customer data, including transaction history and customer profiles. The server is equipped with a high-performance CPU processor and 128GB of RAM, with the current Linux OS version. It utilizes a MySQL database management system and stable network connectivity via IPv4. Security features utilized include SSL/TLS encrypted connections.

Scope

The objective of this vulnerability analysis will be to rectify the database server access controls and the risks associated with it as it has open access. The analysis is included under the umbrella of three months, from June 20XX to August 20XX. The risk analysis will be carried out in line with the NIST SP 800-30 Rev. 1 guidelines.

Purpose

The database server plays a very fundamental role in business infrastructure as it holds valuable data of customers who are accessed by employees for conducting business such as identifying potential customers and processing transactions. Proper safety of the information is very paramount to prevent wrong access, stealing, or changes of customer records.

If the database server is brought down, business operations would be greatly impacted since employees utilize the system to execute day-to-day operations. In addition, customer trust and company reputation could be significantly impacted if sensitive data are leaked.

Risk Assessment

Threat Source\\tThreat Event\\tLikelihood\\tSeverity\\tRisk

Outsider (Hacker)\\tGet sensitive data through exfiltration\\t3 (High)\\t3 (High)\\t9

Privileged user\\tModify/Delete vital customer data\\t2 (Moderate)\\t3 (High)\\t6

Outsider (Hacker)\\tPerform Denial of Service (DoS) attack\\t3 (High)\\t2 (Moderate)\\t6

Outsider (APT)\\tDeploy persistent network sniffers\\t2 (Moderate)\\t2 (Moderate)\\t4

Standard user

Accidentally reveal customer data

2 (Moderate)

2 (Moderate)

4

Method

The vulnerability scan has taken into account a number of factors such as data storage and management, external and internal threats, and business operation risk in the event that these threats are realized. By taking into account the probability and severity of each threat that was realized, we can quantify the overall risk to business operations and data integrity.

Remediation Strategy

Authentication and Authorization: Apply strong authentication policies, including MFA for access to the database. Also ensure role-based access control (RBAC) so that only sanctioned staff can retrieve sensitive data.

Encryption: Encrypt everything in transit with the latest version of TLS protocol (not SSL) to support secure communication among the database server and remote staff.

Access Controls: Restrict access to the database through IP allow-listing, such that only corporate office IP addresses have access to the database. This restricts unwanted access from external sources.

Monitoring and Auditing: Use logging and monitoring to see who accesses the database and what is accessed. Auditing logs should be checked on a regular basis for signs of suspicious use or unauthorized access.

Training of Employees: Educate employees in data security practices and the importance of protecting access credentials, e.g., not sharing password details or falling victim to phishing attacks.

Conclusion

The database server is a company asset with vital customer information. Its existing configuration, public facing, has certain critical vulnerabilities that may result in data breaches, loss of service, and loss of customer trust. The following proposed remediation measures will minimize these risks and help the database server as well as data contained there be secure and uncompromised.

Next Steps

Review and approve the remediation plan that has been suggested.
Implement multi-factor authentication, IP allow-listing, and encrypt the implementation.
Perform vulnerability scanning regularly to ensure continuous security of the system.

By following NIST SP 800-30 Rev. 1 guidance recommendations and remediation of the vulnerabilities, the business can significantly reduce its risk profile and improve overall security posture.