Vulnerability Assessment Report

System Description

The system under assessment is a database server that stores sensitive business information, including customer data, transaction records, and operational metrics. The server is integral to the organization's data management processes and is accessed by authorized personnel through secure internal networks. The primary components include the database engine, data storage, user authentication systems, and network interfaces.

Scope

The scope of this assessment covers the confidentiality, integrity, and availability of the data stored on the database server. It excludes physical security measures and the security of other interconnected IT systems.

Purpose

The primary purpose of this vulnerability assessment is to identify potential security weaknesses in the database server to prevent data breaches and service disruptions. Protecting the server is essential for maintaining business continuity, safeguarding customer information, and ensuring compliance with data protection regulations. Failure to secure this server could result in data loss, financial damage, and reputational harm to the organization.

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk Score
External Attackers	Data exfiltration through SQLi	3	3	9
Insider Threats	Unauthorized data access	2	2	4
Malware	Data corruption via ransomware attack	2	3	6

Approach

This qualitative assessment focuses on identifying high-risk threats by evaluating their likelihood and severity based on the system description and scope. The chosen threats—SQL injection, unauthorized access, and ransomware—represent common vulnerabilities in database servers, posing significant risks to data integrity and availability. These threats were selected based on historical data breaches and known attack vectors targeting similar systems.

Remediation

To mitigate the identified risks, the following security controls are recommended:

1. Implement multi-factor authentication (MFA) for database access to reduce unauthorized entry.
2. Enforce the principle of least privilege by limiting user permissions to the minimum necessary.
3. Apply regular patching and updates to the database server to mitigate known vulnerabilities.
4. Utilize intrusion detection systems (IDS) to monitor for suspicious activity and potential SQL injection attempts.

Conclusion

By implementing the recommended security controls, the organization can significantly reduce the risk of data breaches, unauthorized access, and ransomware attacks, thereby enhancing the overall security posture of the database server.