Vulnerability Assessment Report

Date: July 31, 2024

System Description:

- A remote database server storing company information.
- Accessed by remote employees worldwide for customer data queries.
- Publicly accessible since company launch three years ago.

Scope:

- This assessment focuses on access control vulnerabilities related to the public accessibility of the database server.
- Confidentiality, integrity, and availability of the data are primary concerns.
- Physical security and other IT systems are outside the scope of this assessment.

Purpose:

- The database server is critical for storing valuable customer data used for sales and marketing efforts.
- Securing this data is essential to maintain customer trust, comply with regulations, and prevent financial and reputational damage in case of a breach.
- Unauthorized access could lead to data theft, manipulation, or disruption of business operations.

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk
Outsider (Hacker)	Obtain sensitive information via exfiltration	2 (Moderate)	3 (High)	6
Outsider (Hacker)	Alter/Delete critical information	2 (Moderate)	3 (High)	6
Outsider (Hacker)	Conduct Denial of Service (DoS) attacks	2 (Moderate)	2 (Moderate)	4

Export to Sheets

Approach

The assessment focused on the inherent risks associated with a publicly accessible database server. The likelihood of threat events was evaluated based on the server's exposure to the

internet, the potential motivation of malicious actors, and the absence of adequate access controls. The severity was assessed based on the potential impact on confidentiality, integrity, and availability of sensitive customer data, as well as the potential disruption to business operations.

Remediation Strategy

- Implement strict access controls to limit database access to authorized personnel only. This includes:
    - **Strong Password Policies:** Enforce complex passwords, regular changes, and prevent reuse.
    - **Multi-Factor Authentication (MFA):** Require an additional authentication factor beyond passwords for increased security.
    - **Role-Based Access Control (RBAC):** Grant users access based on their roles and responsibilities.
    - **IP Whitelisting:** Restrict access to specific IP addresses or ranges associated with company locations.
- Upgrade encryption protocols:
    - **Transition from SSL to TLS:** Ensure the use of the latest and most secure encryption protocols for data in transit.
- Continuous Monitoring and Improvement:
    - **Regular Vulnerability Scans:** Conduct periodic scans to identify and address any new vulnerabilities.
    - **Security Awareness Training:** Educate employees on best practices for data security and recognizing potential threats.
    - **Incident Response Plan:** Develop and test a plan for responding to and recovering from security incidents.

Conclusion:

This assessment highlights the significant risks associated with the current configuration of the database server. Implementing the recommended remediation strategies will significantly enhance data security, protect against unauthorized access, and ensure business continuity.

Submitted by: Junaid Shakoor

Date of Submission: July 31, 2024