Vulnerability Assessment Report

ArzSec Cyber Consulting
December 16, 2024
Abbas Raza, Cybersecurity Analyst

Scenario

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

You are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. You must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.

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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database is incredibly important to the business for several reasons. Firstly, it hosts all customer data which employees use to conduct business. Secondly, it allows employees to work remotely; any disruption to this server would have an impact on employees' abilities to get work done.

A security breach for this server would negatively impact the company's ability to conduct business and may harm the company's reputation, leading to further loss of business. Both customers and suppliers may pull their business out of fear of exposure to such a breach. New business prospects may also hesitate to engage with the company.

Executive Summary

The company's database server is currently exposed to the public internet without proper access controls, posing a **critical risk** to confidentiality, integrity, and availability of sensitive data. This report identifies the vulnerability, assesses potential threats, quantifies business impacts, and provides prioritized remediation steps to mitigate risks.

Key Findings:

- Public exposure of the database server increases the likelihood of **data breaches, unauthorized access, and service disruption**.
- Threat actors (e.g., hackers, competitors, disgruntled employees) could exploit this vulnerability to **steal customer data, disrupt operations, or manipulate records**.
- **Severity:** High (Risk scores of 6–9 on a 9-point scale).
- **Recommended Actions:** Immediate implementation of access controls, encryption, and monitoring.

System Description

Hardware: High-performance server (128GB RAM, multi-core CPU).

Software: Linux OS, MySQL database management system.

Network: IPv4, SSL/TLS encryption (needs upgrade to TLS 1.2+).

Current Security Posture:

- No authentication or IP restrictions.
- Publicly accessible since deployment (3+ years).

Risk Assessment

Methodology

Aligned with **NIST SP 800-30 Rev. 1**, risks were evaluated based on:

- **Likelihood (1–3 scale):** Probability of exploitation (3 = Highly Likely).
- **Severity (1–3 scale):** Impact on business (3 = Critical).
- **Risk Score** = Likelihood × Severity

Identified Risks

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Exfiltration of customer/sales data*	*3*	*3*	*9 (Critical)*
Insider	*Unauthorized access or data manipulation*	*2*	*3*	*6 (High)*
Hacker	*Data theft, ransomware, or DoS attacks*	*3*	*3*	*9 (Critical)*

Business Impacts:

- **Financial:** Regulatory fines (e.g., GDPR, CCPA), loss of customer trust.
- **Operational:** Disruption to remote workforce, downtime.
- **Reputational:** Brand damage, loss of business partnerships.

Approach

Potential threat actors were selected based on who would be most likely to take advantage of such a vulnerability. Competitors and former, upset employees would have strong motivation for taking advantage of the open server. Potential hackers would have the technical expertise to be able to act maliciously and would know how to take advantage of this situation.

Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on day-to-day operational needs.

Remediation Strategy

To address the critical vulnerability of the publicly exposed database server, a phased approach is recommended to ensure rapid risk reduction while maintaining operational continuity.

Immediate actions (within 24–48 hours) should focus on restricting access and hardening the system. First, public access to the database must be disabled, and IP allow-listing should be implemented to permit connections only from corporate offices or trusted VPNs. Simultaneously, strong authentication mechanisms—including mandatory complex passwords and multi-factor authentication (MFA)—must be enforced for all users. Additionally, outdated SSL encryption should be replaced with TLS 1.2 or higher to secure data in transit.

In the short term (1–2 weeks), role-based access control (RBAC) should be configured to limit user privileges based on job functions (e.g., read-only access for analysts, write access for managers). Comprehensive audit logging must also be enabled to track all database queries and access attempts, facilitating incident detection and forensic analysis.

Long-term measures (1–3 months) should include regular penetration testing to identify and remediate residual vulnerabilities, along with employee cybersecurity training to mitigate insider threats. Continuous monitoring tools (e.g., intrusion detection systems) and backup/recovery plans should also be implemented to ensure resilience against future attacks.

Compliance & Legal Considerations

GDPR/CCPA: Public data exposure may violate data protection laws, risking fines up to **4% of global revenue**.

PCI DSS: If payment data is stored, compliance failures could lead to **loss of merchant privileges**.

Conclusion

The publicly exposed database is a **severe and urgent risk** requiring immediate action. By implementing the recommended controls, the company can mitigate threats, comply with regulations, and safeguard its reputation.

Next Steps:

- Approve remediation plan and allocate resources.
- Assign IT team to implement IP restrictions and MFA.
- Schedule a follow-up review in 30 days.