REPORT
Server Security Evaluation

v1.2.0

Author:

Eldon Gabriel

July 9, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/14/2025	Eldon G.	Initial draft.
v1.1.0	02/21/2025	Eldon G.	Minor revisions and formatting updates.
v1.2.0	07/09/2025	Eldon G.	Added section headers, numbering, and conclusion.

SECTION 1.0: SERVER SECURITY EVALUATION

1.1 Project Description

I am tasked with evaluating a critical vulnerability in the company's remote database server. It has been open to the public without restrictions since the company started. My job is to identify the risk impact and recommend defensive measures based on NIST SP 800-30 Rev. 1.

1.2 Incident Overview

A global e-commerce company's database server has been open to the internet for three years with no access controls. Employees worldwide frequently access customer and transaction information from this server. This configuration puts sensitive data at risk of being stolen, disrupted, or deletion.

This lack of basic security creates a serious business risk. The next step is to run a vulnerability check and suggest ways to secure the server.

1.3 System Description

- **Hardware**: High-performance CPU with 128GB RAM
- **OS**: Latest Linux distribution
- **Database**: MySQL
- **Network**: IPv4 connectivity, interacts with internal systems
- **Security**: SSL/TLS for encrypted data transmission

1.4 Scope of Assessment

- **Focus**: Access control and data exposure
- **Assessment Period**: June 2024 – August 2024
- **Framework**: NIST SP 800-30 Rev. 1 – Risk Management Guide for Information Systems

1.5 Purpose

The goal is to assess and quantify risks from allowing public access to the company's database server. The aim is to recommend security controls that ensure the confidentiality, integrity, and availability of sensitive customer and business data. This is vital for business continuity, legal compliance, and trust.

SECTION 2.0: 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*

SECTION 3.0: APPROACH

The assessment followed the guidelines from NIST SP 800-30 Rev. 1. I reviewed the access configurations, evaluated the likelihood and severity of potential incidents. I then prioritized risks affecting availability, confidentiality, and integrity.

Main issues found:

- **Open access permissions** on the remote server
- No authentication on access
- No **segmentation** between internal and public areas

SECTION 4.0: REMEDIATION STRATEGY

To lower risk, put these recommended controls in place:

Access Restrictions

- Implement **firewalls** and **Access Control Lists (ACLs)**
- Apply **IP allow-listing** to restrict access to trusted sources

Identity & Authentication

- Use **Multi-Factor Authentication (MFA)**
- Apply **Role-Based Access Control (RBAC)**

Data Protection

- Replace outdated SSL with modern **TLS protocols**
- Encrypt data **at rest and in transit**

Monitoring & Maintenance

- Conduct **regular vulnerability scans**
- Apply **security patches** promptly
- Enable **continuous monitoring and logging**

SECTION 5.0: CONCLUSION

5.1 Key Takeaways

- The publicly accessible configuration is a major security gap with high risk.
- The most critical threats involve data theft, service disruption, and data tampering.
- Current access control mechanisms are insufficient for a global operation handling sensitive data.

5.2 Security Implications and Recommendations

- Immediate lockdown of the database server using network-level controls is critical.
- Implement identity management and logging systems for better accountability.
- Introduce encryption, regular audits, and automated alerting for early breach detection.

By implementing these strategies, the company will reduce its exposure to serious threats and align with best practices from the NIST risk management framework.