Vulnerability Assessment Report

11st January 2025

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 purpose of this vulnerability assessment, as guided by NIST SP 800-30 Rev. 1, is to identify and evaluate security risks associated with the database server, which is integral to the business for managing sensitive information like customer data and transaction records. Securing the data on this server is critical to maintain confidentiality, integrity, and availability, thereby ensuring compliance with relevant regulations and safeguarding the trust of clients. This assessment will also assess the potential impact if the server were to be disabled or compromised, considering the operational disruptions, financial losses, and reputational damage that could ensue. By providing a thorough analysis, it supports strategic security decisions, helping to prioritize risk mitigation efforts, validate the effectiveness of current security measures like SSL/TLS, and enhance the system's resilience against both current and emerging threats.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Business email compromise	*An employee is tricked into sharing confidential information.*	*2*	*3*	*6*
Weak Credentials	*Subject to brute-force attacks.*	*2*	*3*	*6*
Hardware Failure	*Lack of redundancy or backups.*	*2*	*2*	*2*
Misconfigured User Authorization	*Exploiting permissions from a user that shouldn't have access.*	*3*	*3*	*9*
Natural Disasters	*Power outages could lead to lack of accessibility from this service.*	*1*	*3*	*3*

Approach

We selected risks like Business Email Compromise and Weak Credentials based on their prevalence and impact in similar environments. Likelihood and severity scores were derived qualitatively from historical data and expert judgment, with risk values calculated by multiplying these scores. Limitations include reliance on qualitative data, lack of consideration for emerging threats, and the absence of real-time monitoring to account for dynamic changes in the threat landscape.

Remediation Strategy

Before diving into the specific remediation strategies, it's crucial to understand the context of our approach. This vulnerability assessment has highlighted key areas where our database server is at risk, ranging from cyber threats like email compromise and weak credentials to physical risks such as natural disasters. Our strategy aims to not only address these identified vulnerabilities but also to fortify our overall security posture. By implementing targeted, practical, and effective controls, we intend to mitigate these risks, ensuring the integrity, confidentiality, and availability of our critical data. The following remediation strategy outlines actionable steps designed to enhance our security framework, leveraging both existing controls and introducing new measures to adapt to the evolving threat landscape.

- **Business Email Compromise:** Implement advanced email filtering, regular staff training, and enable multi-factor authentication (MFA) for email.
- **Weak Credentials:** Enforce strong password policies, use account lockout, and consider password managers.

- **Hardware Failure:** Establish regular backups, create a disaster recovery plan, and perform predictive maintenance.
- **Misconfigured User Authorization:** Audit user permissions, use automated tools for configuration checks, and implement role-based access control (RBAC).
- **Natural Disasters:** Enhance physical security with environmental controls and update the business continuity plan.

- **Current Controls:** SSL/TLS, basic firewalls, and some user authentication.
- **Security Controls to Reduce Risks:** The proposed controls (MFA, strong passwords, redundancy, RBAC, environmental controls) target each vulnerability directly.
- **Improvement in Security:** These measures will enhance defense against cyber attacks, ensure data availability, control access, and prepare for physical threats, improving overall system resilience.