Vulnerability Assessment Report

1st January 20XX

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 security analyst's vulnerability assessment is to identify and evaluate potential weaknesses within the database server used by the business. This server holds crucial information for employees seeking potential customers, making its security paramount. The assessment aims to safeguard sensitive data, encompassing not only customer details but also employee personal information and other confidential data. By uncovering vulnerabilities, the assessment helps prevent potential threats that could disrupt business operations and mitigate the risk of reputational damage or negative publicity resulting from a successful attack on the server. Ultimately, the assessment supports the company in maintaining data integrity, operational continuity, and a positive public image.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Hacker	*Obtain sensitive information via exfiltration.*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

After a thorough investigation the events that pose a major business risk due to their potential consequences are as follows. The hacker will have unauthorized access through malware could expose sensitive information, leading to competitive disadvantage and legal issues. The cusotme can manipulate data integrity which will disrupt vital operations, causing financial losses and damaging the organization's reputation. Lastly the employee tampering with critical data could disrupt daily processes, hinder decision making, and erode trust among customers and regulators.

Remediation Strategy

To address the identified vulnerabilities, the following steps should be taken. First employee privileged access, implementing role-based access control to restrict employees' access to the database server based on their job responsibilities. Regular access audits should be conducted to ensure access rights are aligned with job roles. Secondly public access control, configure a firewall to restrict public access to the database server. Only authorized IPs should be allowed to connect, and non-essential services should be disabled to minimize attack surface. Third competitor risk mitigation, encrypt sensitive data at rest and in transit to prevent unauthorized access even if the server is compromised. Additionally, implement intrusion detection systems (IDS) to monitor and respond to any suspicious activities. Fourth database security overhaul, conduct a thorough security assessment of the database server to identify and patch vulnerabilities. Regular security updates and patches should be applied promptly to mitigate potential exploits. Lastly, access for departments, set up separate user accounts for employees in different departments with access controls based on the principle of least privilege. Implement a strong authentication mechanism and multi-factor authentication (MFA) for added security. Failure to address these vulnerabilities could lead to severe disruptions in business operations and reputational damage. It's essential to prioritize database security to prevent unauthorized access and potential breaches.