Vulnerability Assessment Report

1st September 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

This assessment aims to identify vulnerabilities in the current database configuration and recommends appropriate security measures. The database server is incredibly valuable to the ecommerce business as it holds critical information about their customers, employees, business partners, suppliers, and more. It also contains analytics data that can be used to customize marketing campaigns and track performance. The goal is to protect the confidentiality, integrity, and availability of their information systems. If the server were disabled for any reason, business operations would be significantly and negatively impacted. Examples of potential impacts would be financial loss, reputational damage, or compliance violations. The security team must protect this data from internal and external threats to keep their day-to-day operations running smoothly and efficiently.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Disrupt mission-critical operations*	*3*	*3*	*9*
Competitor	*Obtain sensitive information via exfiltration*	*2*	*3*	*6*

Privileged User	*Alter/Delete critical information*	*3*	*2*	*6*

Approach

The risks were assessed using the NIST SP 800-30 reference guide. These risk scores were determined by multiplying the likelihood and severity scores of potential security incidents. During this evaluation, I determined that technical and operational controls needed to be scrutinized further. Due to the open access permissions of the company server, cybercriminals, motivated by financial gains or competitive advantage, can easily disrupt and prevent normal day-to-day operations by compromising the confidentiality and integrity of information. This potential security incident poses the highest risk. Moreover, due to lack of access controls, competitors may install malicious software within the organization's information systems to search and acquire sensitive information. Internal threats also pose significant risks. A privileged user can modify or delete data, intentionally or unintentionally, potentially causing critical damage to company data or assets and significantly impacting business operations.

Remediation Strategy

It would behoove this company to focus their efforts on technical controls first. I strongly recommend the organization implement MFA to authenticate users who are attempting to access company resources and systems data. I also recommend implementing PKI to encrypt sensitive information. Additionally, I encourage the company to verify the identity of all public key holders to further shield against the exfiltration or manipulation of sensitive data via authentication. Furthermore, I suggest that the company properly configure a firewall and set rate limits in order to remediate potential DoS attacks. These security hardening techniques can significantly limit the hacker's ability to disrupt business operations and reduce the threat of a competitor using private and sensitive company data to their advantage.

In addition to these technical controls, an operational control that can be implemented includes the principle of least privilege. Limited and proper database access for only those employees who require it for their job functions addresses the risk of data modification, deletion, or exfiltration by privileged users. Another operational control can include quarterly access reviews. By conducting routine reviews to verify that permissions remain appropriate, the company can promptly revoke user access for those who no longer need access.