Vulnerability Assessment Report

2024

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

Purpose:

The database server is a centralized computer system that stores and manages large amounts of data. This data can include sensitive information such as customer records, financial transactions, and proprietary business information.

Securing the data on the server is paramount for several reasons. First and foremost, it protects confidentiality by safeguarding sensitive information from unauthorized access and potential breaches. Additionally, ensuring the integrity of data is vital for operational effectiveness, as accurate and reliable data underpins critical business decisions. Compliance with legal and regulatory requirements related to data protection and privacy is also

essential, as failure to adhere to these standards can result in significant penalties.

Finally, maintaining customer trust and safeguarding the company's reputation is crucial; preventing data leaks not only protects the organization but also fosters confidence among clients and stakeholders. Overall, a robust data security strategy is integral to the success and longevity of the business.

If the server were disabled, the business could experience significant disruptions, including a loss of access to critical data and services, which would lead to operational inefficiencies. This downtime could also result in potential financial losses due to halted transactions and service interruptions. Additionally, the organization's reputation and customer trust would suffer, potentially causing long-term damage to business relationships. Overall, the consequences of server downtime can be far-reaching and detrimental to the company's success.

Risk Assessment:

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	Obtain sensitive information via exfiltration	3	3	9
Employee	Disrupt mission-critical operations	3	3	6
Customer	Alter/ Delete critical information	1	3	3
Natural Disaster	Server downtime due to physical damage	2	4	6
Malware	Data breach via malicious software	4	5	9

Approach:

Risks that were measured considered the data storage and management procedures of the business. 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. Limitations of the assessment included the inability to perform penetration testing due to operational constraints and the reliance on existing documentation, which may not capture all security vulnerabilities.

Remediation Strategy:

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

The current security controls in place consist of several layers designed to protect the system. Technical controls include the use of SSL/TLS for data encryption, robust firewalls, and regular software updates to address vulnerabilities. Operational controls focus on user access management and monitoring database activities to detect any suspicious behavior. Additionally, managerial controls are implemented through comprehensive security policies and training programs aimed at educating staff about data protection practices. Together, these controls form a multi-faceted approach to safeguarding the system and its sensitive data.

The recommended security controls aim to strengthen the system's overall security posture. First, implementing enhanced access controls through role-based access controls (RBAC) will limit access based on job functions, ensuring that only authorized personnel can access sensitive data.

Additionally, conducting regular security audits, including periodic vulnerability assessments and penetration testing, will help identify and mitigate risks proactively. Developing and testing a comprehensive incident response plan is crucial for effectively addressing potential data breaches or server downtime. Finally, increasing employee awareness through training on recognizing phishing attempts and other security threats will further bolster the organization's defenses against cyber risks. Together, these measures will significantly improve the system's security and resilience.

Improving Overall Security:

Implementing the above recommendations will strengthen the security posture of the system, mitigate identified risks, and enhance the ability to respond to future threats. Continuous monitoring and improvement of security practices will ensure ongoing protection of sensitive data and maintain business continuity.

Conclusion:

This vulnerability assessment underscores the critical importance of securing the database server to protect the integrity and confidentiality of business data. By addressing identified risks and implementing the recommended remediation strategies, the organization can significantly enhance its overall security framework.