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

- As the newly appointed cybersecurity analyst for our e-commerce company, I have conducted a vulnerability assessment of our remote database server and identified crucial issues that demand immediate attention. Our database server holds essential data crucial for day-to-day operations, making it highly valuable to our business. However, its current state of being open to the public poses significant risks. Unauthorized access to sensitive data could lead to identity theft, financial fraud, and intellectual property theft. Additionally, a data breach could result in loss of customer trust, compliance violations, and legal penalties. If the database server were disabled, it would disrupt our operations, lead to revenue loss, and damage our reputation. To address these risks, I recommend implementing strong authentication, access controls, encryption, regular security audits, and network segmentation, along with data backup and disaster recovery protocols. These measures will bolster our cybersecurity posture and ensure the safety of our business and customer data.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Malicious External Actors	*Malicious external actors with the intent to cause harm or gain*	*5*	*5*	*25*

	unauthorized access could exploit the open database server to steal sensitive customer information, payment data, or intellectual property			
Disgruntled Employees, Ex-employees, Contractors with unauthorized access	*Insiders who have legitimate access to the database server could pose a significant threat if they misuse their privileges or become disgruntled. Disgruntled employees or ex-employees may attempt to steal sensitive data, compromise the server, or leak valuable information*	*4*	*4*	*16*
Misconfigured Access Controls, Weak Passwords, Negligent Employees	*Human errors within the organization can inadvertently expose the database server to potential risks. Misconfigured access controls or weak passwords might make it easier for unauthorized individuals to gain access*	*3*	*3*	*9*
Customer	*Alter and delete important information*	*1*	*2*	*2*

Approach

The three specific threat sources/events I selected are malicious external actors, insider threats, and unintentional human errors. These threats are significant business risks due to their potential impact on our open database server. Malicious external actors, such as cybercriminals and nation-state actors, pose a serious risk of data breaches, financial fraud, and reputational damage. Insider threats, including disgruntled employees or contractors, can exploit their legitimate access to the server to steal sensitive information or disrupt operations. Unintentional human errors, like misconfigured access controls or weak passwords, can inadvertently expose the server to unauthorized access and data leaks. Addressing these

threats is essential to protect our business operations, customer data, and overall reputation as a secure and trustworthy e-commerce company.

Remediation Strategy

The remediation strategy for addressing the vulnerabilities associated with the open database server involves a comprehensive and multi-layered approach. We will enhance security measures by implementing strong access controls, such as multi-factor authentication and role-based access, to ensure that only authorized personnel can access the server. Sensitive data will be protected through data encryption both at rest and in transit, and anonymization of certain fields will be considered to minimize the risk of exposing personally identifiable information. Regular security audits and vulnerability scanning will be conducted to proactively identify and address weaknesses in our system. Additionally, we will prioritize employee training and security awareness programs to educate our staff about cybersecurity best practices, reducing the risk of insider threats and unintentional human errors. Lastly, we will establish a comprehensive incident response plan and disaster recovery plan to swiftly address security incidents and ensure business continuity in case of severe breaches. By adopting this approach, we will fortify our database server, protect our valuable data, and reinforce our commitment to providing a secure and reliable e-commerce platform.