Vulnerability Assessment Report

21st July 2023

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 April 2023 to June 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is vital to ensure the continued success, trustworthiness, and stability of the e-commerce business. It is a centralized computer system used for the storage of data. The data stored comprises crucial business operations' data. This data includes customer data, business intelligence data, and analytical data. As such, the data must be protected to ensure privacy and confidentiality is maintained in accordance with regulatory practices.

It is important to secure the data on the server, as the e-commerce company has employees who work remotely from all around the world. Although the employees may be of good character, implementing a zero-trust policy will ensure that we verify the security of the database. Additionally, it would be beneficial to secure this data to comply with legal and regulatory legislation (e.g., depending on the data: PCI-DSS, GDPR, PII, SPII, and HIPAA), which in return will build customer trust. Ensuring that the data server is secure will also protect intellectual property. Doing so will keep the competitors from conducting corporate espionage. Lastly, securing the database server can prevent any insider (e.g., disgruntled employees) or outsider threats from gaining access and performing malicious or otherwise harmful activities to the database.

In the event that the server is disabled, the business would be severely impacted. The results would be a loss of productivity/revenue loss, customer unhappiness/reputational damage, and costs to remediate including legal fees or fines resulting from a data leak.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employee – insider threat	*Alter data or delete in a way that negatively impacts the company or intentionally steal data.*	***2***	***3***	***6***
Competitor, Supplier, Business Partner – outsider threat	*Conduct corporate espionage by obtaining sensitive information via exfiltration.*	***3***	***3***	***9***
	Alter data or delete in a way that negatively impacts the company or intentionally steal data.	***1***	***3***	***3***
	Obtained sensitive data via data breach is released to the public.	***3***	***3***	***9***
Hacker – outsider threat	*Alter data or delete in a way that negatively impacts the company or intentionally steal data.*	***3***	***3***	***9***
	A certificate authority is compromised to make connections appear legitimate.	***3***	***2***	***6***
	Overtime, the threat source examines and assesses the company's vulnerabilities using various tools (e.g., scanning, physical observation).	***3***	***2***	***6***
	Overtime, the threat source installs software designed to collect network traffic.	***3***	***2***	***6***
	Threat source conducts a Denial of Service (DoS) attack to overwhelm the system's operating capabilities.	***3***	***3***	***9***
	Threat source injects SQL	***3***	***3***	***9***

	commands to query the database server.			
	Threat source conducts a man-in the-middle attack to eavesdrop on a private connection.	*3*	*2*	*6*
	Threat source enables persistence by putting a backdoor into the server.	*3*	*3*	*9*
Customer – insider threat	*Alter data or delete data in a way that negatively impacts the company, or intentionally steal data.*	*1*	*3*	*3*

Approach

The risks considered consisted of a combination of internal and external human and technological risks. The main threat sources for the remote database server used for the e-commerce business that conducts operations globally were customers, hackers, competitors, suppliers, business partners, and employees.

The risks were determined by assessing the likelihood of a threat occurrence and the impact of the potential threat events. As the database server is open to the public, the likelihood and severity of the risks were mostly high.

Remediation Strategy

Recommended remediation strategies for the public database server are as follows:

- Implement authentication, authorization, and auditing (AAA) practices using strong password policies, role-based access controls (RBAC), multi-factor authentication (MFA), and periodic security audits and penetration tests to identify vulnerabilities and weaknesses in the database server's security posture.
- Encrypt data in transit using TLS instead of SSL and encrypt data at rest with compatible encryption algorithms. Require remote access users to connect to the database server over a Virtual Private Network (VPN).
- Deploy a database firewall to prevent SQL injections and block unused ports.

- Implement IP allow-listing to corporate offices to prevent non-company IP addresses connecting to the database.
- In addition to periodic audits, continuous monitoring using Intrusion Protection Systems (IPS) should be used to respond to threats promptly.
- Ensure known good backups are maintained and checked regularly. Also, implement a Disaster Recovery Plan/ Business Continuity Plan.
- Regularly administer cybersecurity awareness and security training for employees.