Vulnerability Assessment Report

7th February 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. The assessment will cover a period of three months, from August 2023 to November 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

- *The company stores potential customer information on the database server*
- *The data on the server needs to be secured to protect the PII of customers and employees.*
- *A disabled server would cease all services and would be a potential loss to the organization.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacktivist	*Conduct Denial of Service (DoS) attacks.*	*3*	*3*	*9*
Employee	*Alter/Delete critical information*	*2*	*3*	*6*

Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

- *A hacktivist, depending on what their motives are, would most likely cause a catastrophic event if the database server is set to public.*
- *A company employee, without a set access control and sufficient training, could accidentally alter and delete crucial information.*
- *A hacktivist would most likely occur since they are constantly trying to make a statement while a company employee would be a less frequent occurrence. Both threat sources would initiate a catastrophic security event.*
- *The limits to this assessment is only through human factors since the technological and environmental aspect is negligible due to only a period of three months with updated equipment.*

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

- *The system 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.*
- *Several security controls can help reduce the risks evaluated. These are:*
    - *Implement Network Segmentation: By isolating the database server within a dedicated network segment, you can minimize the exposure of the server to potential threats from the public internet.*
    - *Implement Intrusion Detection and Prevention Systems (IDPS): IDPS solutions provide proactive threat detection and response capabilities, helping identify and mitigate security incidents such as unauthorized access attempts, malware infections, and suspicious network activities.*
    - *Regular Security Assessments and Audits: proactively identify and address potential security risks and vulnerabilities before they can be exploited by attackers.*

- By implementing these security controls, you can significantly reduce the risks associated with keeping the database server open to the public and enhance the security posture of the e-commerce company's infrastructure. These controls help protect the confidentiality, integrity, and availability of the company's sensitive data and minimize the impact of potential security incidents and breaches.