Vulnerability Assessment Report

24th 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 June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The purpose of this report is to ensure that the database server is secured to reduce the attack surface as the organisation relies heavily on the remote database server to store information as many of the employees work remotely from home around the world. It is used regularly by organisational staff to query and request data from the server to find potential customers.

It is important for the organisation to secure the data on the server to protect the data information that is stored on the server, to comply with regulations that are in place regarding data protection, protect the information security of employees, and to protect the reputation of the organisation. Unsecured data can lead to massive implications if a breach occurs.

If the server was disabled, it would impact the organisation by potential data loss, the organisation could also face legal consequences for failing to protect the data stored, and cause damage to the organisation's reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*

Insider Threat	*Unauthorised data access and leak*	*2*	*4*	*8*
Phishing Attempts	*Compromising employee's credentials*	*3*	*3*	*9*

Approach

The selection of the three threat sources and events were based on analysis of potential risks to the organisation, due to the current cybersecurity landscape and characteristics of the organisation. Employees with access to the database server can accidentally or intentionally misuse sensitive information stored, which poses a risk to confidentiality of data and potentially harm the organisation's reputation.

Phishing emails or websites can trick employees into giving credentials to threat actors, which would lead to unauthorised access to the server and result in data breaches.

Competitors attempting to obtain sensitive information via exfiltration can result in loss of competitive advantage as they can use data to undermine our organisation, and can cause damage to customer trust as their data was not safeguarded and can result in legal and regulatory consequences.

Remediation Strategy

Enforce the principle of least privilege across the organisation, maintaining that employees are only able to access what they are required to have to perform their role.

The database should not be made public, and ensure that a robust AAA framework is implemented to control access to the server, and that authenticated users with proper authorisation can access specific resources, whilst the accounting logs provide user activities for monitoring and auditing purposes.

Encrypting sensitive data on the server by implementing a Public Key Infrastructure to enhance encryption, secure communication, and verifying authenticity of users.

Regular Security Awareness training for all employees to help educate them on common phishing techniques and social engineering attacks to help recognise and avoid potential threats, which will reduce the likelihood of employees falling victim to phishing attacks.