Vulnerability Assessment Report

1st January 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 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 assessment is to establish the vulnerability of the remote database server which stores data for ecommerce. This remote server is valuable because many of the employees work in multiple global locations where they can query or request data in order to find potential customers; its protection is vital to standard business operations.
It is important for the business to secure the data on the server because threat actors may implement changes to data or steal data in order to negatively impact business operations. Alternatively, there may be technical or environmental factors that may cause the server to fail, such as aging equipment, resource depletion or a compromised operational environment. If the server was disabled the business may fail in its duty to keep data private and may lose data altogether, leading to a critical disruption in business operations and perhaps further reputational consequences.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Conduct DoS attack to overwhelm*	*2*	*3*	*6*

	the system's operating capabilities.			
Hardware	*Database is compromised due to hardware failure - aging server for example.*	*1*	*3*	*3*

Approach

In the risk assessment, competitor exfiltration, hacker DoS attack and hardware failure have all been identified. This is because the severity of impact is significant (all scoring 3). While likelihood remains relatively low to moderate, the normal functioning of business operations will be compromised to the point of complete disruption, and additionally when considering competitor exfiltration, theft of private data. This would lead to reputational damages as well as compromised business continuity, both with the potential to cause financial loss.

Remediation Strategy

Considering the server has been public since its first implementation three years ago it would first be recommended to implement access controls that follow the AAA principles (authentication, authorisation and accounting). First, multi-factor authentication can be implemented in order to verify access to a legitimate user - this could be biometric data as well as a username/password strategy. Similarly one-time passwords can be implemented to strengthen access controls. In terms of authorisation a strategy based on the principle of least privilege and a separation of duties would mean that data can only be accessed by those who need it, and no one individual will need access to all data. All these authorisation strategies might support the safety of the current remote working model. Furthermore, accounting strategy could include monitoring data logs to examine for suspicious activity including unusual login behaviour, particularly important in the remote working model. Defense-in-depth strategies focusing on **1)** perimeter protection, such as a perimeter filter to oversee incoming and outgoing traffic, **2)** network protection such as a firewall, **3)** endpoint protection such as antivirus software may help protect from malicious actors conducting exfiltration or DoS attacks. It could also be recommended to implement public key infrastructure (PKI) tactics for example, implementing the use of public and private keys to address exfiltration of data, in this instance, by a competitor.