Vulnerability Assessment Report

20th 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 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server is critical to the continuing operation of the business, as it is required for many globally based employees to fulfill their roles. The server or the data contained within becoming unavailable or damaged would constitute a critical cybersecurity incident because it would lead to many employees being unable to perform their duties. It is also important that the data on the server is kept secure as it includes the personally identifiable information (PII) of customers.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Disgruntled Employee	*Alter/Delete critical information*	*3*	*3*	*9*
Server Failure	*Disrupt mission-critical operations*	*1*	*2*	*2*
Competitor	*Obtain sensitive information via exfiltration.*	*3*	*2*	*6*

Approach

The altering or deletion of data by a disgruntled employee was identified as a critical risk due to the lack of access controls to manage the availability of data stored on the server. Given the public access to the server, any threat actor with motivation is able to view and alter data at will.

The exfiltration of sensitive data by a competitor was also identified as medium-risk. While it would be easy for a competitor to gain access to data stored on the server given the publicly available access, the data is already in the public domain and would thus be of limited value to a competitor.

Hardware failure of the server itself was also identified as a risk, however this is considered to be a low-risk scenario. This is because the server has appropriate physical resources (i.e. CPU, memory etc.) as well as a stable and secure connection to the rest of the network.

While these risks have been identified, a more thorough assessment cannot be conducted without greater access to the organisation's network and preferably elevated access to the server itself.

Remediation Strategy

It is recommended that the organisation implement security controls around access to the server to ensure that the principle of least privilege (PoLP) is being followed. Employees should not have access to data that is not required to perform their usual duties, and data should not be accessible to the public. Given that the workforce is spread over a large geographical area and is therefore difficult to monitor, multi-factor authentication (MFA) should also be introduced to verify the identity of users. Access privileges should be regularly audited to ensure that privilege-creep does not occur. These controls will improve the organisation's security posture by ensuring defense in depth and an appropriate authentication, authorisation and accounting (AAA) framework.