Vulnerability Assessment Report

1st January 20XX

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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

The database server allows the business to communicate with other servers on the network, and hosts a SQL database management system. It is important to secure the data on the server, since a large volume of it will be vulnerable to interception while it is in transit. Data could be compromised by threat actors looking to tamper with packets, or IP spoofers looking to impersonate individuals from the company. If the server were to be disabled, the business would not be able to access the internet, or connect with any cloud-based services, and any transactions involving customers and clients would come to a standstill.

Risk Assessment

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

Advanced persistent threat	*Perform reconnaissance and surveillance of organization*	*2*	*2*	*4*
Employee	*Conduct DoS attack*	*3*	*3*	*9*
Hacker	*Conduct “man in the middle” attacks*	*2*	*3*	*6*

Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

Three potential threat sources present significant business risks in the case that they trigger a threat event. APTs, threat-acting employees, and hackers were selected as major threats to the business server, which is susceptible to attacks involving data packets in transit, during the TCP handshake protocol, and when IP addresses are compromised through IP spoofing. These attacks could lead to stolen PII or SPII, compromised internal-only business practice information, and even a complete halt in business operations that can cost large amounts of financial loss. It is therefore highly important that safeguards are implemented to reduce the likeliness of these events, securing the day-to-day successful operations of the company.

Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

Encription of data in transit

Monitoring network traffic/ Threat-detaction software