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

The database is constantly being used by employees who work remotely from locations all around the world to find potential customers. The database has the customers data, and analytic data that can later be used to track personalised marketing efforts. Without the server, the company will not be able to maintain business continuity and may lose customers.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*
Competitor	*Conduct Denial of Service attacks*	*2*	*3*	*6*

Approach

Risks that were measured considered the data storage and management procedures of the business. Due to the fact that the database is public, mainly external threat sources and events were chosen for the assessment. Sensitive information may be stolen using exfiltration or man-in-the-middle attacks for financial gains as the business is an e-commerce. Competitors may want to do a DoS attack on the business to disrupt business continuity.

Remediation Strategy

The AAA framework should be implemented to ensure that only authorised users access the database server to prevent customers from being able to alter/delete critical information. There should be back-up servers and properly configured firewalls with port filtering to prevent the DoS attacks. Finally, IDS should be set up to monitor the network and search for known threats and suspicious or malicious traffic to better detect any exfiltration attempts.