Vulnerability Assessment Report for an e-commerce company

System Description

The server uses a powerful CPU processor and 128GB of memory. It's using the latest linux operating system. The OS is hosting a MySQL database management system, and, to ensure stable connections during interaction with other servers, it is using IPv4. For secure transmission, it's using SSL/TLS connections.

Scope

The scope of the assessment will cover the current access controls being deployed. The assessment will run for 3 months, from June 2022 to August 2022 and during the assessment, the NIST SP 800-30 will be used as a guide to analyse information systems

Purpose

The database is the core of the business, without the database, the business would struggle. The remote workers use the database to find potential customers, it holds critical and sensitive information about potential customers.

It's important that organisations secure their databases, because they contain potential customers data, which competitors may try to access. Also, unauthorised access could lead to data being altered or deleted.

If the server was disabled, the business would struggle, new customer leads wouldn’t be able to be stored and all the remote workers' momentum would come to a grinding stop.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information	1	3	3
Threat Actor	Delete/Alter	2	3	6
Insider Threat	Financial Gains	3	2	6

Approach

The market is saturated, therefore being a market leader in such an environment comes with challenges. Competitors could spend their resources on trying to obtain valuable information from the database to advance their ranking. The likelihood of this happening is low however the severity is high.

Threat actors pose a major risk to the database. Unauthorised access could allow them to delete or alter data, compromising its availability and integrity.

Insider threats (employees) level of access could potentially be exploited. Employees could use the data for financial gains if they have no professional integrity.

Remediation Strategy

To ensure the confidentiality, integrity and availability of information in the database, robust security measures need to be taken. The current security controls are inadequate and present huge risks. Some of the security controls that can be implemented are Role based access controls, multi factor authentications and encryption such as TLS instead of SSL.

-