Vulnerability Assessment Report

(eCommerce Company)

System Description

A remote machine used a database server for storing the company's data. This server is accessed by multiple people from different locations, globally. Currently, it's being maintained as an open resource for anyone who wishes to access it.

Scope

The scope of this analysis consists of evaluating the potential risks involving the remote data server used by the company. The goal of this report is to assess, score, and propose possible solutions to the risks surrounding the asset in question. The NIST SP 800-30 document will be used as a reference for this assessment.

Purpose

As previously stated, the goal of this evaluation is to determine the possible risks involving a valuable asset to the company. This server stores the company's customers' PII, internal-only information, and confidential information regarding business operations, such as data used to direct marketing strategies.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Employees	Data access, alteration, and deletion can be performed by any employee. A mistaken disclosure, alteration or deletion of the data can be done by anyone.	*3*	*3*	*9*
	As mentioned before, the asset is placed in a high level of exposure, which means that it is also highly			

Hackers	susceptible to malicious entities, such as hackers. A threat with the level of computer knowledge that hackers have, can certainly impose higher risk to the machine, which leads to profound damage to the asset, the company's reputation and business operation.	*3*	*3*	*9*
Customers or anyone with knowledge about the server	The server is open for public view, which means that the customers can have access to the data. But not only them, any entity with knowledge about the existence of this exposed server can have access to it as well. This level of exposure leads to data modification, deletion or disclosure by anyone.	*2*	*3*	*5*
Virus infection	The data server is also at risk of virus infection, just like any other computer. Since the machine is not used as a regular computer for checking emails and accessing websites, the most likely problem regarding virus infection is the purposely installation of malicious software, which can be performed by anyone with access to the machine, in this case unsatisfied customer with knowledge about the server, a current or ex employee with bad intentions or hackers.	*2*	*3*	*5*

Approach

The way through which the risks were assessed was by considering the possible vectors that could be exploited by malicious users and entities with access to the system, and as previously stated, the report used as reference the NIST SP 800-30 documentation in order to score and review possible malicious sources.

The *likelihood* score was done based on business operation and how the asset is involved during the operation, if the machine has more exposure to a specific kind of threat, the score was set higher for likeness. Furthermore, the *severity* score was based on the level of impact that could be experienced by the company in the event of an attack to the server, the bigger the impact, the higher the score.

However, the report has limitations to its investigation due to the lack of further information regarding asset. For example, it wasn't disclose the exact physical location of the computer, this information would have been of great importance for assessing physical risks to the system. There was also no information about the use of cloud services in the machine, which would also influence the addition of more risk to the assessment and a slightly different approach regarding the strategies to secure the system.

Remediation Strategy

The first step to reduce the *severity* of the risks, it's to reduce the exposure of the server. Diminishing the level of access to the system will reduce some of the risks but it will also entirely remove some of the possible threats.

Other security measures should be implemented as well. The use of authorization and authentication to secure the system is paramount, implementing security barriers such as MFA (Multi Factor Authentication) and principles such as *least privilege* and *separation of duties* will come in great addition for securing the asset.

Monitoring and keeping track of the access to the database is also something to be considered. Together with that, the implementation of secure communication protocol via internet and remote access is vital, TLS and SSH, respectively, are recommended. Listing the allowed ip who have access to the system is another security layer to be placed, since many employees of the company work remotely, this will guarantee that unwanted entities don't have access to the system.

Security measures regarding the data store in the server should be looked into as well. Implementing salted hashing algorithms for securing passwords and using encryption to transfer data from and to the system are some of those measures. Policies for creating strong passwords have to be placed in order for the hashing to work properly.

Finally, to ensure all the protective measures are working as intended and are being properly implemented, periodic security audits should be performed at the company. This will

guarantee compliance to the internal regulation set by the company, and it will also be a great way to start complying to external regulation needed to avoid fines and damage to the company's reputation.