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 server is a valuable asset to the business. It contains sensitive information and could be exploited by threat actors in many ways, such as reputational damage, identity fraud, and for financial gain. It is important to secure this to mitigate the risks against the aforementioned threats, as well as ensure compliance with legal regulations regarding protecting and safeguarding sensitive information. The company holds customer data on this database server, and it therefore must be protected properly. If the server were disabled, workers would not be able to access critical information to perform their job function. Service disruptions and downtime can also impact the organization's reputation and lead to financial damages.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Human - Competitor	*A competitor is able to access information on the public database, and use it for a competitive advantage.*	*2*	*3*	*6*
Human - Hacker	*A hacker is able to access information on the public database, and uses the sensitive customer data for identity fraud.*	*3*	*3*	*9*
Technological - Hardware	Company details: 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. The organization is using powerful and up to date hardware and software. Threat event is hardware failure due to aging.	*1*	*3*	*3*
Human - Employee	Employees are regularly querying or requesting information from the database. There does not appear any kind of least privilege strategy in place. This could be exploited if an employee was compromised.	*2*	*3*	*6*

Approach

The first threat source, a competitor of the organization, gaining access to sensitive customer information. With this information, they may use it for a competitive market advantage, or to even harm the reputation of the business. This can also be said for the second threat source, a hacker, who could compromise this public database and use the information for further harm, like identity theft or financial fraud. Employees are regularly requesting information or querying the database. It is likely that there is no implementation of least privilege, which leaves massive vulnerabilities and widens the attack surface of the company.

Remediation Strategy

Implementing the principle of least privilege, would shorten the attack surface in the event an employee is compromised by a threat actor. Securing the database so that only authorized users could access it would also mitigate risks or unauthorized access. Thus keeping sensitive information more secure. Employees requesting information should also be approved/denied appropriately, meaning that they should only be requesting and given access based on their job function.