Vulnerability Assessment Report

26th June 2024

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 is very important to the business because it stores information that employees all over the world can use to find potential customers. Securing the data on the server can prevent damages to the business in several ways, for example protecting the company's reputation and trust from the customer. It also prevents the business from violating government regulations that can lead to heavy penalties like fines. And lastly it also helps maintain the continuity of the business or even grow the business. Since the server is accessed by many employees from multiple places all over the world, if the database server were disabled it would be difficult to contain the damage as the data is already spread across the world. Another issue that may arise from this is it can completely stop the operation of the business until the database is restored to its functioning state.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk

Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Alter/Delete critical information*	*2*	*3*	*6*
Networking	*Conduct DoS 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.

Exposing the database server to the public makes it easier for competitors and hackers to understand the infrastructure, the design, and more information about the server. Gaining this information makes it easier for these two threat sources to attack the server and cause damages to the business. The competitor might try to steal the business's customer's information and try to find a better marketing strategy to attract these potential customers. Hackers can also steal the customer's information for the intention of identity theft, or cause further damage to the business by altering or deleting critical information. Lastly, since the server is still using IPv4 instead of IPv6 and considering that the server is being accessed from all over the world, the database server is more prone to DoS attacks.

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.

Properly configuring the firewall as well as regularly updates the rules for the firewall to prevent threat actors from attacking the server

Updating the server to use IPv6 instead of IPv4 to reduce the chances of DoS attacks

And lastly is implementing encryption to the database so in case the server is compromised the attacker still can't access the information contained in the server.