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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*

  El servidor de de la compañía, contiene la base de datos que almacena los datos de todos sus clientes por lo tanto es un activo de alto valor.

- *Why is it important for the business to secure the data on the server?*

  Es sumamente crítico que la empresa proteja estos datos, debido a que en cualquier momento un agente de amenaza podría percatarse de esto y comprometer la confidencialidad, integridad y disponibilidad de la información sin ningún problema, podría provocar daños irreparables, arriesgándose a pérdida de reputación y además a multas por el mal manejo de datos sensibles. Esto pondría en gran peligro la continuidad del negocio dado a que cualquier contrincante podría obtener beneficio de esto.

- *How might the server impact the business if it were disabled?*
  La empresa podría ver afectada en su totalidad la correcta funcionalidad de sus operaciones, debido a que gran parte de sus empleados trabaja de forma remota con el servidor, por lo tanto significaria grandes pérdidas, además de daños graves y filtración de datos.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Hacker	*Install persistent and targeted network sniffers on organizational information systems*	*3*	*3*	*9*
Competitor	*Disrupt mission-critical operations.*	*1*	*3*	*3*

Approach

Se han seleccionado estas tres vulnerabilidades debido a la forma en que la empresa administra y guarda sus datos, dado a que su servidor se encuentra completamente abierto, cualquiera podría escanear los puertos con acceso y ejecutar exploits para extraer información sensible de sus clientes o de la compañia, ademas podrian instalar sniffers de redes para capturar todo el tráfico y así obtener información de los movimiento que hacen los trabajadores dejándolos expuestos a ellos y sus dispositivos a cualquier ataque. Por otro lado un competidor mal intencionado que identifique como amenaza a la compañía, podría entrar con facilidad a los sistemas y entorpecer sus operaciones para beneficio propio.

Remediation Strategy

Implementación de mecanismos de autenticación, autorización y auditoría para garantizar que solo los usuarios autorizados accedan al servidor de la base de datos. Esto incluye el uso de contraseñas seguras, controles de acceso basados en roles y autenticación multifactor para limitar los privilegios de los usuarios. Cifrado de datos en movimiento mediante TLS en lugar de SSL. Listado de direcciones IP permitidas en las oficinas corporativas para evitar que usuarios aleatorios de internet se conecten a la base de datos. Es fundamental la implementación de PKI que permiten la comunicación segura, la autenticación de usuarios y dispositivos, y la protección de datos mediante el cifrado.

Además se debe implementar el uso de Hashes para el correcto almacenamiento de datos, deben ser encriptados y salteados, sino la información de los usuarios y la compañía quedará

expuesta de todas formas, además si no se utilizan hashes cualquiera podría instalar malware y nadie se percataria a tiempo.