Informe de evaluación de vulnerabilidad

1calleEnero de 20XX

Descripción del sistema

El hardware del servidor consta de un potente procesador y 128 GB de memoria. Funciona con la última versión del sistema operativo Linux y aloja un sistema de gestión de bases de datos MySQL. Está configurado con una conexión de red estable mediante direcciones IPv4 e interactúa con otros servidores de la red. Las medidas de seguridad incluyen conexiones cifradas con SSL/TLS.

Alcance

El alcance de esta evaluación de vulnerabilidades se refiere a los controles de acceso actuales del sistema. La evaluación abarcará un período de tres meses, de junio de 20XX a agosto de 20XX.NIST SP 800-30 Rev. 1Se utiliza para guiar el análisis de riesgos del sistema de información.

Objetivo

Considere las siguientes preguntas para ayudarle a escribir:

- *¿Qué valor tiene el servidor de base de datos para el negocio?*
- *¿Por qué es importante para la empresa proteger los datos en el servidor?*
- *¿Qué impacto podría tener el servidor en el negocio si se deshabilitara?*

Evaluación de riesgos

Fuente de amenaza	Evento de amenaza	Probabilidad	Gravedad	Riesgo
Por ejemplo, competidor	*Obtener información sensible mediante exfiltración*	*1*	*3*	*3*
Empleado	*Extracción de la base de datos*	*2*	*3*	*3*
Encargado de IT	*No encriptar base de datos*	*1*	*3*	*3*

Acercarse

Los riesgos consideraron los métodos de almacenamiento y gestión de datos de la empresa. La probabilidad de ocurrencia de una amenaza y el impacto de estos eventos potenciales se compararon con los riesgos para las necesidades operativas diarias.

Estrategia de remediación

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.