Informe de evaluación de vulnerabilidad

1 de enero de 20XX

Descripción del sistema

El hardware del servidor consta de un potente procesador de CPU y 128 GB de memoria. Se ejecuta en 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 SSL/TLS.

Alcance

El alcance de esta evaluación de vulnerabilidad se relaciona con los controles de acceso actuales del sistema. La evaluación cubrirá un período de tres meses, desde junio de 20XX hasta agosto de 20XX. NIST SP 800-30 Rev. 1 se utiliza para guiar el análisis de riesgos del sistema de información.

Propósito

Considere las siguientes preguntas para ayudarlo a escribir:

¿Qué valor tiene el servidor de base de datos para la empresa?

Es la base de todo, necesitamos los datos para tener la información requerida y modificar/borrar si es necesario. Además con ello tienes un control de los recursos que se trabajan.

¿Por qué es importante para la empresa proteger los datos en el servidor?

Conlleva prestigio, seguridad y confianza de la empresa. Nadie pondría su dinero o cosas de valor en un lugar donde todo el mundo roba por poner un ejemplo.

¿Cómo podría afectar el servidor a la empresa si se deshabilita?

No dar servicio hace perder dinero, y clientes e incluso futuros clientes al ver que las cosas no van bien. Por ello debes dar una imagen de si tienes problemas saber resolverlos o si los tienes resolverlos lo antes posible.

Nota: Los puntos importantes tomando en cuenta en este proceso fueron por parte del servidor y la base de datos. Ya que conllevan mucha importancia, su control debe ser adecuado en todo momento y por ello siempre se deben revisar para no exponerlos a ni un peligro innecesario. Además de la importancia a vista de clientes.

Evaluación de riesgos

Threat source	Threat event	Likelihood	Severity	Risk
hacker	*Obtener datos de la base de datos*	*1*	*3*	*3*
trabajadores	*No tener las suficientes herramientas para mantener los datos*	*2*	*2*	*4*
DDoS	*Intentar denegar servicios*	*2*	*3*	*6*

Nota: estos escenarios no son de los mas peligrosos pero pueden conllevar perder prestigio y clientes, configurar puntos claves en el servicio es importante para evitar cierto tipo de ataques o minimizar la capa de ataque.

Enfoque

Se consideraron los riesgos relacionados con los métodos de almacenamiento y gestión de datos de la empresa. Se sopesa la probabilidad de que se produjera una amenaza y el impacto de estos posibles eventos frente a 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.