Coop. Agricola Mixta Montecarlo Ltda. 2024-09-26 #1 Evaluación de Vulnerabilidades

Escenario

La coop. almacena información en un servidor de base de datos remoto, ya que muchos de los empleados trabajan a distancia y/o desde lugares de toda la provincia. Los empleados de la empresa consultan, o solicitan, regularmente datos del servidor para encontrar clientes potenciales.

La base de datos ha estado abierta al público desde la digitalización de la coop. hace catorce años. Como profesional de la ciberseguridad, se reconoce que mantener el servidor de la base de datos abierto al público es una vulnerabilidad grave.

Se me encomiendo completar una evaluación de la vulnerabilidad de la situación para comunicar los riesgos potenciales a los responsables de la toma de decisiones en la coop.

Se creará un informe escrito que explique cómo el servidor vulnerable supone un riesgo para las operaciones de la coop. y cómo se puede asegurar.

Descripción del sistema

El hardware del servidor consta de 4 servidores Dell PowerEdge™ 2950 III servidores en rack 2S, C/U con 8 ranuras DIMM de almacenamiento completo en búfer para lograr un total de hasta 64 GB de RAM, dos procesadores Intel® Xeon® de cuatro núcleos y una variedad de opciones de interfaz de red, además de hipervisores integrados configurables entre entre VMware®, Citrix® y Microsoft®.

Se ejecutan en la última versión del sistema operativo Linux CentOS para servidores 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 vulnerabilidades se relaciona con los controles de acceso actuales del sistema.

La evaluación cubrirá un período de tres meses, desde Julio de 2024 hasta Septiembre de 2024.

La norma [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) se utiliza para guiar el análisis de riesgos del sistema de información.

Propósito

Preguntas que complementan la decisión de evaluación:

Qué valor tiene el servidor de base de datos para la coop.?

Por qué es importante para la coop. proteger los datos en el servidor?

Cómo podría afectar el servidor a la coop. si se deshabilitara?

El servidor de base de datos es un sistema informático centralizado que almacena y administra grandes cantidades de datos. El servidor se utiliza para almacenar datos de clientes, campañas y análisis que luego se pueden analizar para realizar un seguimiento del rendimiento y personalizar las iniciativas de marketing.

Es fundamental proteger el sistema debido a su uso habitual para operaciones de marketing.

Evaluación de riesgos

| **Fuente de la Amenaza** | **Evento de Amenaza** | **Probabilidad** | **Gravedad** | **Riesgo** |
| --- | --- | --- | --- | --- |
| Hacker | Obtención de información sensible vía exfiltración | 3 | 3 | 9 |
| Empleado | Interrumpir operaciones de misión crítica | 2 | 3 | 6 |
| Cliente | Modificar/eliminar información crítica | 1 | 3 | 3 |

Enfoque

Los riesgos se midieron considerando los métodos de almacenamiento y gestión de datos de la coop.

Las fuentes y eventos de amenazas potenciales se determinaron utilizando la probabilidad de un incidente de seguridad dados los permisos de acceso abierto del sistema de información.

La gravedad de los incidentes potenciales se evaluó frente al impacto en 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 de la cooperativa y otras instalaciones para evitar que usuarios aleatorios de Internet se conecten a la base de datos.