UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FIME
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA
APLICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN AD2023

GRUPO:

033

SALÓN:

3105

NOMBRE DEL MAESTRO:

Susana Gabriela De La Cruz Mauricio

NOMBRE DEL ALUMNO:

Obed Jacobo Flores Sepúlveda

MATRÍCULA:

2178104

CARRERA:

Administrador de Sistemas

FECHA:

16/11/2023

LUGAR:

Cd. Universitaria, San Nicolás de los Garza, N.L.

Índice

Introducción

En la actualidad digital, asegurar la integridad de los datos se ha convertido en un desafío esencial para organizaciones en todo el mundo. La creciente dependencia de la tecnología de la información y las comunicaciones ha ocasionado un incremento significativo en la cantidad de datos manejados por las empresas. Sin embargo, este aumento también ha llevado consigo un incremento en las amenazas cibernéticas y la vulnerabilidad de los sistemas de información. En este artículo, examinaremos la problemática de la gestión de la seguridad de datos y cómo un Ingeniero Administrador de Sistemas puede desempeñar un papel crucial en su resolución.

Desarrollo

La protección de datos ha emergido como una temática de considerable relevancia en la actualidad, siendo motivada por diversos elementos. En primera instancia, el incremento exponencial en la magnitud de datos almacenados y gestionados por organizaciones ha generado un terreno propicio para la materialización de ataques cibernéticos. Los datos, catalogados como el activo más preciado de una entidad, se encuentran en la mira de amenazas cibernéticas, y su extravío o compromiso podría desencadenar repercusiones catastróficas, incluida la pérdida de la confianza del cliente y la afectación de la reputación corporativa.

En segundo lugar, la complejidad de los modernos sistemas de información ha experimentado un marcado incremento. Las empresas hacen uso de una diversidad de tecnologías y plataformas para la administración de sus datos, abarcando desde servidores locales hasta soluciones en la nube y aplicaciones móviles. Esta variabilidad de sistemas crea brechas potenciales en términos de seguridad que los perpetradores cibernéticos pueden aprovechar.

En tercer lugar, las amenazas cibernéticas están en un constante proceso de evolución. Los actores maliciosos emplean tácticas cada vez más sofisticadas para evadir las defensas tradicionales, transformando la seguridad de datos en un desafío perpetuamente cambiante. Adicionalmente, los Ingenieros Administradores de Sistemas (IAS) también pueden incurrir en errores, de los cuales detallaremos algunos, junto con los puntos a considerar para su resolución:

Abuso de la escalada de privilegios: Se pueden aplicar estrategias como la administración cuidadosa de cuentas privilegiadas y la restricción de acceso a archivos y directorios.
Uso de software desactualizado: Resulta esencial evaluar parches tan pronto como estén disponibles, poner en cuarentena servidores cuando no sea posible aplicar una actualización crucial y asegurar que la administración comprenda la importancia de las actualizaciones.
Deficiente gestión de contraseñas: Medidas como evitar el uso de la misma contraseña de root en todas las máquinas, asegurar la robustez de las credenciales de administrador y evitar almacenar contraseñas en archivos de texto son cruciales.
Solución de problemas de asignación incorrecta de VLAN: Se puede abordar este problema mediante la reconfiguración de puertos para adaptarse a nuevos servicios, la

validación de la nueva asignación de VLAN mediante la revisión de la configuración del conmutador y la verificación de la compatibilidad de VLAN mediante pruebas de puertos.

- **Supervisión de archivos de registro en busca de señales de manipulación y ataque**: Estrategias como registrar información en dos ubicaciones distintas, evitar la inclusión de contraseñas o intentos fallidos de acceso en registros y la utilización de software de filtrado de registros son cruciales para identificar información relevante.
- **Conflicto de direcciones IP**: Se recomienda verificar conflictos de IP que puedan surgir de servidores, evaluar políticas BYOD y realizar la liberación y renovación de direcciones IP.
- **Ineficiente gestión de claves SSH**: Aspectos como supervisar la rotación de claves SSH, vincular claves SSH a individuos específicos en lugar de cuentas compartidas y mantener un inventario detallado de todas las claves SSH son esenciales.

La contribución de los Ingenieros Administradores de Sistemas en la resolución de los desafíos relacionados con la seguridad de datos en entornos organizativos es de suma importancia. A continuación, se detallan diversas formas en las que estos profesionales pueden aportar:

Diseño y Mantenimiento de Infraestructura Segura: Los Ingenieros Administradores de Sistemas desempeñan un rol crucial en la concepción, implementación y mantenimiento de la infraestructura tecnológica de una organización. Este ámbito abarca servidores, redes y sistemas de almacenamiento. Al integrar principios de seguridad desde las etapas iniciales, pueden asegurar que la infraestructura sea robusta frente a amenazas cibernéticas.

- **Gestión de Identidad y Acceso**: El control preciso sobre quién tiene acceso a los sistemas y datos es esencial para garantizar la seguridad. Implementando sistemas de Gestión de Identidad y Acceso (IAM), los Ingenieros Administradores de Sistemas pueden asegurar que únicamente las personas autorizadas tengan acceso a información crítica.
- **Monitoreo y Detección de Amenazas**: Los Ingenieros Administradores de Sistemas tienen la capacidad de establecer sistemas de monitoreo continuo, detectando actividades sospechosas o intrusiones. La detección temprana desempeña un papel crucial en la mitigación del impacto de posibles ataques.
- **Actualización y Parcheo**: El mantenimiento de sistemas y software actualizados es esencial para cerrar posibles vulnerabilidades conocidas. La responsabilidad de aplicar parches de seguridad y actualizaciones de manera regular recae en los Ingenieros Administradores de Sistemas.
- **Educación y Concientización**: Los ingenieros pueden desempeñar un papel significativo en la educación y concientización de los empleados en cuanto a prácticas seguras en línea. Esto abarca la capacitación en temas como el phishing, contraseñas seguras y otros aspectos relacionados con la ciberseguridad.

- **Administración, Integración y Configuración de Sistemas de Tecnología de Información**: Estos profesionales no solo administran, sino que también integran y configuran sistemas de tecnología de información. Esto implica la gestión de recursos humanos, financieros y técnicos, participando activamente en el desarrollo de conocimientos científicos y tecnológicos, aplicando estándares de calidad y promoviendo la mejora continua.

Conclusión

La administración efectiva de la seguridad de datos representa un desafío crítico en el actual contexto digital. Los Ingenieros Administradores de Sistemas ocupan una posición singular para afrontar esta problemática al concebir, implementar y preservar sistemas y medidas de seguridad sólidas. Su pericia técnica y habilidades en la gestión de sistemas de información resultan inestimables para salvaguardar los recursos más cruciales de una entidad: sus datos. A medida que las amenazas cibernéticas siguen evolucionando, la contribución de los Ingenieros Administradores de Sistemas se torna aún más esencial para el triunfo y la continuidad operativa de las empresas en el entorno digital.

Bibliografía

Universidad Autónoma de Nuevo León. (2018, agosto 2). Ingeniero Administrador de Sistemas. UANL - Universidad Autónoma de Nuevo León. https://www.uanl.mx/oferta/ingeniero-administrador-de-sistemas/

Santana, C. (2022, abril 11). 10 errores comunes de seguridad que cometen los administradores de sistemas y cómo evitarlos. Cristian Thous - Ciberseguridad al alcance de todos. https://cristianthous.com/10-errores-comunes-de-seguridad-que-cometen-los-administradores-de-sistemas-y-como-evitarlos