Estrategias de seguridad en base de datos

Percy Taquila
Epis - UPT
percy-taquila23@hotmail.com

Edward Apaza
Epis - UPT
edward-123@hotmail.com

1. ABSTRACT

Un problema común de seguridad a todos los sistemas de computo es el evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información, efectuar cambios mal intencionados en la totalidad o una porción de la base de datos. Se presentan algunas reglas básicas para empezar a gestionar la seguridad en el diseño e implementación de una base de datos.

A common security problem for all computer systems is to prevent unauthorized persons from accessing the system, either to obtain information, to make ill-intentioned changes in the whole or a portion of the database. Some basic rules are presented to start managing security in the design and implementation of a database.

Keywords: base de datos, gestión, seguridad, algoritmos de cifrado.

2. INTRODUCCION

Un problema común de seguridad a todos los sistemas de computo es el evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información, efectuar cambios mal intencionados en la totalidad o una porción o totalidad de la base de datos.

La ciberdelincuencia se define como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático.

Las bases de datos no protegidas son el sueño de cualquier cyber delincuente. Contienen los datos más valiosos de la organización, blanco fácil de un ataque y que están convenientemente organizados. No es de extrañar que las bases de datos sean el objetivo principal de los cyber ataques.

3. OBJETIVO

Entender la importancia de seguridad en la base de datos.

4. MARCO TEORICO

4.1. Concepto de Base de datos

- Es un conjunto de datos que pertenecen al mismo contexto, almacenados sistemáticamente para su uso posterior.
- Conjunto de información relacionada que se encuentra agrupada o estructurada.

4.2. Características

- Independencia lógica y física de los datos. - Redundancia mínima. - Acceso concurrente por parte de múltiples usuarios. - Integridad de los datos. - Consultas complejas optimizadas. - Seguridad de acceso y auditoría. - Respaldo y recuperación. - Acceso a través de lenguajes de programación estándar.

4.3. Sistema de Gestión de Base de Datos (SGBD)

Los Sistemas de Gestión de Base de Datos (en inglés DataBase Management System) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

4.4. Ventajas de las bases de datos

Control sobre la redundancia de datos: Los sistemas de ficheros almacenan varias copias de los mismos datos en ficheros distintos. Esto hace que se desperdicie espacio de almacenamiento, además de provocar la falta de consistencia de datos.

Compartir datos: En los sistemas de ficheros, los ficheros pertenecen a las personas o a los departamentos que los utilizan. Pero en los sistemas de bases de datos, la base de datos pertenece a la empresa y puede ser compartida por todos los usuarios que estén autorizados.

Mejora en la integridad de datos: La integridad de la base de datos se refiere a la validez y la consistencia de los datos almacenados. Normalmente, la integridad se expresa mediante restricciones o reglas que no se pueden violar. Estas restricciones se pueden aplicar tanto a los datos, como a sus relaciones, y es el SGBD quien se debe encargar de mantenerlas.

4.5. Tipos de Base de datos

SEGÚN LA VARIABILIDAD DE DATOS ALMACENADOS:
- Estáticas: los datos que contiene son solo de lectura. Básicamente se utiliza para almacenar datos históricos.
- Dinámicas: Puede realizarse operaciones sobre los datos que contiene, entre ellas: consulta, actualiacion, adición y eliminación.

SEGUN EL CONTENIDO:
- Bibliográficas: Su contenido es solo una representación de la fuente primaria.
- Numéricas: Almacena datos numéricos.
- Bases de texto completo: Estas pueden almacenar el contenido completo de una publicación.

4.6. Modelos de Base de datos

BASE DE DATOS JERÁQUICAS: Almacenan su información en una estructura jerárquica, representando los datos en forma de árbol, donde un nodo padre de información puede tener varios hijos. Este modelo es bastante útil cuando la cantidad de información es pequeña.

BASE DE DATOS EN RED: Los datos se representan como colecciones de registros y las relaciones entre los datos se representan mediante conjuntos, que son punteros de la implementación física. Este sistema permite que un nodo tenga más de un padre.

BASE DE DATOS RELACIONAL: Se utiliza para modelar los problemas reales y administrar datos dinámicamente.

BASE DE DATOS ORIENTADA A OBJETOS: Este modelo es uno de los más recientes, almacena en la base de datos tanto el estado como el comportamiento del objeto. Algunas de las propiedades de este modelo son: la encapsulación (Permite ocultar la información al resto de objetos, para impedir accesos incorrectos o conflictos); herencia (los objetos heredan comportamiento dentro de una jerarquía de clases) y poliformismo (permite que una operación pueda ser aplicada a distintos tipos de objetos).

BASE DE DATOS DOCUMENTALES: Permite realizar diferentes actividades sobre el texto, una de las más importantes es la búsqueda de texto, que se puede realizar dentro de un documento.

5. ANALISIS

5.1. Técnicas de seguridad

El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo. Ésto, se denomina control de acceso y se pone en practicas creando cuentas de usuarios y contraseñas para que es SGBD controle el proceso de entrada al sistema.Otra técnica de seguridad es el cifrado de datos, que sirve paraproteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado provee protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo ex profeso. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contará con algoritmos (o claves) de codificación o descifrado para tal efecto.

5.2. Los usuarios

Deberían tener varios tipos de autorización para diferentes partes de la base de datos. Destacan:
- La autorización de lectura para la lectura de los datos,pero no su modificación.
- La autorización de inserción para la inserción de datos nuevos, pero no la modificación de los existentes.
- La autorización de actualización para la modificaciónde los datos, pero no su borrado.
- La autorización de borrado para el borrado de los datos.

5.3. Prácticas de seguridad

IDENTIFIQUE SU SENSIBILIDAD: Desarrolle o adquiera herramientas de identificación, asegurando éstas contra el malware, colocado en su base de datos el resultado de los ataques de inyección SQL; pues aparte de exponer información confidencial debido a vulnerabilidades, como la inyección SQL, también facilita a los atacantes incorporar otros ataques en el interior de la base de datos.

EVALUACIÓN DE LA VULNERABILIDAD Y LA CONFIGURACIÓN: Esto incluye la verificación de la forma en que se instaló la base de datos y su sistema operativo (por ejemplo, la comprobación privilegios de grupos de archivo -lectura, escritura y ejecución- de base de datos y bitácoras de transacciones).

Además, es necesario verificar que no se está ejecutando la base de datos con versiones que incluyen vulnerabilidades conocidas; así como impedir consultas SQL desde las aplicaciones o capa de usuarios. Para ello se pueden considerar (como administrador):
- Limitar el acceso a los procedimientos a ciertos usuarios.
- Delimitar el acceso a los datos para ciertos usuarios, procedimientos y/o datos.
- Declinar la coincidencia de horarios entre usuarios que coincidan.

ENDURECIMIENTO: Como resultado de una evaluación de la vulnerabilidad a menudo se dan una serie de recomendaciones específicas. Estees el primer paso en el endurecimiento de la base de datos. Otros elementos de endurecimiento implican la eliminación detodas las funciones y opciones que se no utilicen. Aplique una política estricta sobre que se puede y que no se puede hacer, pero asegúrese de desactivar lo que no necesita.

AUDITE: Una vez creada la configuración y controles de endurecimiento, realice auto evaluaciones y seguimiento a las recomendaciones de auditoría para verificar la no desviación de su objetivo (la seguridad).Automatice el control de la configuración de tal forma que registre cualquier cambio en la misma e implemente alertas sobre cambios en ella. Cada vez que un cambio se realice, podría afectar a la seguridad de la base de datos.

SUPERVISIÓN: Supervisión en tiempo real de la actividad de base de datos es clave para limitar su exposición, aplique o adquiera agentes inteligentes de monitoreo, detección de intrusiones y uso indebido.

PISTAS DE AUDITORIA: Aplique pistas de auditoría y genere la trazabilidad de las actividades que afectan la integridad de los datos, o la visualización los datos sensibles.

6. CONCLUSIONES

- Debemos emplear toda las técnicas necesarios para poder hacer que nuestra base de datos este segura.
- Los datos de cualquier organización son una propiedad muy valiosa.
- Las bases de datos son un objetivo favorito de los cyber ataques debido a la importancia de los datos.

References

[1] Seguridad de base de datos. https://es.slideshare.net/mesarango/bd-avanzada-video

[2] Seguridad de datos: En que consite? https://www.powerdata.es/seguridad-de-datos

[3] Seguridad de datos: En que consite? http://ri.ufg.edu.sv/jspui/bitstream/11592/6822/3/005.756-Ch512d-Capitulo

[4] Principios básico de seguridad en base de datos https://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos