Universidad de Costa Rica

Tarea 4

Mario Quirós Luna – B76090

Administración de Bases de datos

Resumen Cap. 14: Seguridad en las bases de datos.

Conceptos básicos de seguridad de la base de datos.

Los DBA son los responsables de administrar la seguridad de la base de datos, algunas organizaciones transfieren esta tarea a un grupo de administración de seguridad aparte que controla la seguridad de toda la compañía.

La autenticación solida es la piedra angular de cualquier plan de implementación de seguridad. Se puede otorgar recursos de base de datos, es necesario establecer un inicio de sesión para cada usuario del DBMS. Los inicios de sesión a veces se denominan cuentas o ID de usuario, tendrá una contraseña asociada de modo que solo aquellos que conozcan la contraseña puedan usar la ID.

Cuando un usuario no necesita conectarse más a una base de datos o deja la empresa el DBA debe eliminar su inicio de sesión lo antes posible, sin embargo, no es posible borrarla si el usuario está usando una base de datos o si el usuario a creado objetos en la base de datos, por esta razón es aconsejable limitar que solo los DBA puedan crear objetos.

Algunos DBMS proporcionan controles y parámetros adicionales sobre inicios de sesión y contraseñas, como un numero de intentos fallidos antes de que se bloquee la cuenta, número de días que una contraseña es válida, reutilización de contraseñas.

Autoridad otorgante y revocatoria

El DBA controla la seguridad y autorización de la base de datos mediante el lenguaje de control de datos o DCL, este es uno de los tres subtipos de SQL, los otros son DDL y DML. Las sentencias DCL se utilizan para controlar que usuarios tienen acceso a que objetos y comandos, el DCL comprende dos tipos básicos GRANT para asignar permiso a un usuario y REVOKE quita un permiso.

Tipos de privilegios

Cada DBMS proporciona ciertos tipos básicos de privilegios como la capacidad de acceder a datos, crear objetos de base de datos y realizar funciones del sistema. Estos

privilegios son comúnmente otorgados por los DBMS modernos: Tabla para controlar quien puede acceder y modificar los datos dentro de las tablas, Objeto para controlar quien puede crear nuevos objetos y eliminarlos, Sistema para controlar quien puede realizar ciertos tipos de actividades en todo el sistema y procedimiento almacenado para controlar quien puede ejecutar funciones específicas y procedimientos almacenados.

Conceder el PUBLIC

Cuando se concede un privilegio a PUBLIC, el DBA pierde el control sobre ese objeto o recurso de la base de datos, volver a obtener el control del recurso será bastante difícil. Se debe reservar al uso de la autoridad PUBLIC para esos pocos objetos y recursos de la base de datos que deberían estar disponibles para todos.

Informes de seguridad

El DBA deberá monitorear e informar sobre los privilegios de los usuarios. Algunos DBMS proporcionan vistas y procedimientos almacenados en el sistema que simplifican la recuperación de la seguridad de la base de datos. Solo el DBA, SA y el administrador de seguridad requieren acceso a la información de seguridad de la base de datos almacenada en el catálogo del sistema.

Roles y grupos de autorización

Además de otorgar privilegios individuales, el DBMS puede proporcionar la capacidad de asignar privilegios específicos a un rol que luego se otorga a otros o grupos de privilegios incorporados específicos.

Una vez definido un rol, se puede utilizar para otorgar uno o más privilegio.

Administrador de sistema (SA), posee la mayor cantidad de privilegios en el DBMS. Un usuario SA puede ejecutar todos los comandos de la base de datos y acceder a todas las bases de datos y objetos.

Administrador de la base de datos (DBA), otorga todos los privilegios sobre una base de datos específica, puede acceder, pero no modificar los datos dentro de las tablas de esa base de datos.

Mantenimiento de la base de datos, incluye privilegios específicos de la base de datos para mantener los objetos de la base de datos (como la capacidad de ejecutar utilidades y emitir comandos).

Administrador de seguridad, permite otorgar y revocar la seguridad de la base de datos en todo el DBMS, puede realizar cualquier acción relacionada con la seguridad.

Control de operaciones (OPER), posee autoridad para realizar tareas operativas de la base de datos, como Backup y recuperación, o finalizar tareas fuera de control.

Otros mecanismos de seguridad de base de datos

Uso de vistas para seguridad

La mayor parte de la seguridad de la base de datos se realiza utilizando la seguridad nativa del DBMS. Sin embargo, es posible simplificar algunos aspectos de la seguridad de lavase de datos creando vistas para proteger sus datos.

Uso de procedimientos almacenador para seguridad

Los procedimientos almacenados se pueden utilizar para proporcionar un nivel adicional de seguridad. Los procedimientos almacenados pueden codificarse para acceder solo a subconjuntos de nivel de fila o columna. Además de proporcionar un nivel de seguridad, este método puede proporcionar un mejor rendimiento si los algoritmos del procedimiento se codifican correctamente.

Cifrado

El cifrado es un proceso mediante el cual los datos se transforman con un algoritmo para que nadie pueda leerlo sin la clave de cifrado. El cifrado ha sido utilizado por gobiernos y organizaciones militares durante años para permitir la transición y comunicación secreta de datos.

Auditoria

La auditoría es una función de DBMS que permite a los DBA realizar un seguimiento del uso de los recursos y privilegios de la base de datos.

La auditoría rastrea lo que ha hecho un usuario en particular una vez que se le ha permitido el acceso.

La auditoría ocurre después de la actividad; no hace nada para prohibir el acceso.

La auditoría también se puede utilizar para la recuperación de datos.

Resumen

La seguridad es uno de los componentes mas importantes en una organización y la labor principal del DBA. Sin una base de datos con la seguridad necesaria para el negocio, la organización estaría completamente comprometida a cualquier tipo de ataque o robo de datos. El DBA debe estar a la vanguardia de cualquier mecanismo de seguridad que sea útil para proteger los datos y la empresa.