**Amenazas y contramedidas que afectan al SGBD**

Los datos son uno de los activos más valiosos para las empresas a día de hoy este es el motivo por lo que la seguridad de estos ha saltado a un primer plano, las empresas cada vez almacenan más datos y de carácter más sensible en los SGBD, la pérdida o corrupción de estos datos podría suponer grandes pérdidas tanto de dinero como de reputación para una empresa.

Las amenazas a las que se somete un SGBD son innumerables, estas amenazas se clasifican conforme las áreas de incidencia que afecten, estas áreas son: robo y fraude, pérdida de confidencialidad, pérdida de la privacidad, pérdida de la integridad y pérdida de disponibilidad.

Una amenaza implica cualquier suceso que pueda afectar negativamente a un sistema y como hemos dicho antes son muchísimas las que un SGBD se puede encontrar, pero no todas las amenazas conllevan el mismo riesgo para el sistema, es por esto que las empresas se centran en buscar solución para las más serias o que más puedan afectar a su organización.

A continuación, citaremos algunas de las amenazas más importantes que pueden afectar a nuestro sistema:

Una de las áreas más afectadas por amenazas de seguridad es el apartado de usuarios que acceden a las bases de datos, aquí pueden surgir todo tipo de amenazas, robo de credenciales para un uso posterior, abuso de privilegios por parte de una cuenta, permisos excesivos, etc. Esta área es extremadamente sensible ya que cualquiera de estas amenazas citadas afecta a casi todas las áreas de incidencia, la pérdida de confidencialidad, privacidad y disponibilidad, así como el robo y fraude son consecuencias inevitables de estas vulnerabilidades ya que afectan al acceso de los datos y dependiendo de los permisos que se hayan visto comprometidos, nos podemos enfrentar a modificaciones, borrado o corrupción de estos.

También son usuales problemas derivados de riesgos físicos a los que se puede enfrentar el hardware, incendios, desastres naturales, daños físicos a los equipos… Todos estos escenarios son plausibles y ponen en gran peligro constante la disponibilidad e integridad de los datos.

Como en todo sistema informático, existe la posibilidad de que los SGBD se vean comprometidos ya sea por puertas traseras, hackeos o escuchas. No solo esto, si no que los sistemas o redes sobre los que están desplegados estos SGBD pueden verse comprometidos, pero esto no nos ocupa en este punto ya que solo prestaremos atención al terreno sobre el que administra la seguridad el SGBD.

Ahora que hemos visto las Amenazas más importantes que acechan a un SGBD, vamos a ver que mecanismos de defensa implementan estos sistemas para protegerse de dichas amenazas.

Comenzamos por el control de autorización, este proceso tendrá como resultado la concesión de un privilegio de acceso a la “persona” autorizada, este proceso conlleva una autenticación mediante unas credenciales. Por lo general, la creación de las cuentas de usuario individuales es tarea del administrador de la base de datos pero

La contramedida anterior va de la mano con la siguiente a tratar, el control de acceso, este se basa en la concesión y revocación de privilegios. Este es un área muy importante ya que, si se utiliza debidamente, resulta en un buen mecanismo de seguridad, pero si no se restringen debidamente los permisos, este mecanismo puede convertirse en una vía libre para vulnerabilidades. Los privilegios deberían ser concedidos de manera que solo se hiciese efectiva la concesión de uno si el usuario que lo recibe no puede hacer su trabajo sin él. Hay distintas formas de implementar este control de acceso, el estándar SQL sigue un control de acceso discrecional o DAC en el que los permisos fluyen desde el propietario de un objeto a quien se crea oportuno mediante las palabras reservadas GRANT y REVOKE. También se puede seguir un control de acceso obligatorio o MAC basado en políticas de nivel de sistema y clases de seguridad que determinan si cierto usuario es apto o no para el acceso o modificación de determinados datos. Este modelo impone dos restricciones, Read-down que restringe a tener una clase de seguridad mayor que el objeto a leer para poderse acceder a este y Write-up que restringe la escritura de un objeto si el sujeto no tiene la misma clase de seguridad o menor.

Las vistas son otra de las contramedidas integradas por el SGBD para evitar los robos de información y la pérdida de privacidad y confidencialidad. Las vistas son tablas virtuales creadas como respuesta a una solicitud. Estas vistas son creadas con el fin de ocultar partes de la información a según qué usuarios de forma transparente, esto es, que el usuario no perciba que se está produciendo dicha ocultación. Esto es posible porque a un usuario se le pueden otorgar permisos sobre una vista y no sobre las tablas base, de esta forma se puede restringir aun más el acceso a las tablas de datos. Estas vistas son creadas por los administradores y se basan en una consulta select que definirá los contenidos de dicha vista.

Para enfrentarse a las pérdidas de integridad y maximizar la disponibilidad de los datos los SGBD integran un sistema de copia de seguridad y recuperación, esta funcionalidad hace posible la recuperación del sistema tras un fallo. Este servicio implica la creación de copias de seguridad de forma periódica en intervalos que vayan en función de las necesidades de la organización que lo implemente. Además de la copia en sí, también se guarda un archivo de las operaciones que se han ido realizando desde la última copia, gracias a estos dos elementos se puede llegar fácilmente hasta una recuperación prácticamente integral (hasta el último estado coherente).

De la mano de las copias de seguridad se encuentra la redundancia, también centrada en maximizar la disponibilidad de los datos y preservar la integridad de estos. Estás técnicas son fundamentales ya que los errores del hardware son prácticamente inevitables y es importante asegurar el servicio incluso cuando estos fallan. Una de las soluciones más usadas de este tipo es la tecnología RAID, su forma de operar se basa en la redundancia de discos físicos de forma que la información se pueda almacenar replicada. Hay diversas formas de distribuir estos datos y sus respectivos metadatos, las variantes más avanzadas de esta tecnología implementan un esquema de paridad para asegurar la integridad de los datos además de la redundancia.

No tanto como para recuperar la integridad de los datos, si no para mantenerla el SGBD cuenta con controles y restricciones de integridad varios. El primero es el de datos requeridos o el exigir que una columna tenga datos válidos no nulos o sí (NULL – NOT NULL). El segundo control consiste en restricciones de dominio para ciertas columnas (CHECK ()). El tercero o Integridad de entidades, el cual dictamina que la columna de la clave principal de una tabla no puede contener valores varios o nulos. El cuarto y último exige la integridad referencial, es decir, que los valores de las claves foráneas deben coincidir con sus valores en las tablas donde son clave principal.

La persecución por preservar la confidencialidad de los datos nos lleva a la siguiente contramedida, el cifrado. El cifrado se encarga, mediante un algoritmo de encriptación, de que los datos no sean legibles por ningún programa o sujeto que no tenga la clave. MySQL en si mismo emplea el cifrado para las contraseñas de los usuarios que existen en la base de datos y el algoritmo de cifrado usado por defecto es un hash SHA-2. Se pueden utilizar tanto algoritmos de cifrado simétrico como asimétrico dependiendo del nivel de seguridad deseado y los detalles logísticos de la organización. Si se aplica cifrado sobre los valores de una tabla hemos de tener en cuenta que el rendimiento de la base de datos en cada consulta se verá afectado ya que el proceso de encriptado y desencriptado ha de ser tenido en cuenta y ralentizará las consultas.

**Seguridad de un SGBD en entornos WEB**

Si la seguridad a nivel de base de datos ya es complicada cuando bajamos a nivel de red se hace aún mas difícil. Las comunicaciones en internet se realizan sobre un protocolo TCP/IP, este protocolo no fue ideado para ser seguro y si no se toman las medidas necesarias los datos pueden ser fácilmente interceptados por un agente externo. Para lograr una comunicación segura en internet de manera que la transmisión y recepción de datos no se vea comprometida, esta comunicación debe seguir 5 principios: confidencialidad, integridad, autenticidad, no simulación y no repudio. Aun siguiendo todos estos pasos, un sistema puede verse atacado, existen ataques de todo tipo, inyección de código SQL, cross-site scripting (XSS), usurpación de credenciales, etc…

Por ello los mecanismos de seguridad de los que hemos hablado en el punto anterior no son suficientes, para proteger al sistema contra las amenazas de la web y así hacerlo accesible desde esta, hay que implementar medidas adicionales.

Es muy común en las organizaciones que se instalen servidores proxy, esta medida mejora el rendimiento de la aplicación a la vez que la seguridad. El servidor almacena las consultas recientes esto hace que las consultas sean respondidas más rápidamente y se ahorren accesos a disco los cuales son muy importantes en sistemas que manejen un volumen muy grande de peticiones. En el apartado de seguridad el servidor proxy contribuye en cuanto a que filtra las peticiones que tienen como destino el SGBD, de esta forma se restringen peticiones indebidas y se pueden implantar restricciones de conexión para evitar ataques al sistema.

La siguiente contramedida tiene que ver en ambientes empresariales en los que existan redes internas, un requisito fundamental en las bases de datos es que se intente en la medida de lo posible mantener el SGBD desconectado de redes de esta índole ya que si dicha red se viese comprometida pondría en peligro la seguridad de toda la base de datos. Es por esto que se implementan cortafuegos para restringir accesos no autorizados a los datos desde o hacia redes privadas, estos pueden implementarse como software o como hardware. Por lo general se implementan mediante diferentes técnicas, la más usual es el filtrado de paquetes, pero también puede por ejemplo utilizarse un servidor proxy como los mencionados en el punto anterior, a modo de cortafuegos si se sitúa entre un SGBD y la red privada.

Estos puntos son sumamente importantes para la seguridad del SGBD, pero sin duda el punto más importante para poder hacer nuestra BD disponible en la red es establecer un canal seguro para la comunicación con esta. Aquí es donde entra en juego la capa de sockets seguros o SSL (Secure Sockets Layer), esta tecnología nos permite cifrar los datos que se transmiten en una conexión mediante algoritmos de cifrado. Cuando una conexión HTTP se realiza sobre SSL se dice que se está siguiendo el protocolo HTTPS o HTTP seguro. Estos protocolos se encargan de hacer posible que el cliente y servidor se autentiquen entre si y validen la información transmitida. Dependiendo de las necesidades logísticas y de confidencialidad de la organización que se esté tratando se utilizaran unas técnicas u otras de autenticación y cifrado, se pueden emplear tanto firmas digitales como certificados expedidos por una Autoridad de certificación en la que ambas partes de la comunicación confían.

Por último, es importante volver a destacar en este punto la importancia del cifrado, en este caso el hasheo de las contraseñas de los usuarios. Los usuarios están almacenados en una tabla del servidor y van a ser un claro objetivo de hackers es por esto que debemos protegerlas. Pongamos un supuesto, nuestro sistema se ve comprometido por un ataque de inyección de código SQL, el atacante ha conseguido ejecutar una consulta SELECT en nuestro sistema y ha conseguido visualizar la tabla usuarios, si nuestras contraseñas no estuviesen cifradas podríamos enfrentarnos a un problema mucho mayor.