Universidad de La Laguna
Escuela Técnica Superior de Ingeniería Informática

Asignatura: BASES DE DATOS

BASES DE DATOS SEGURAS

Alumnos:
Borja Barrera Villagrasa alu0100498820
Yeray Pérez Peraza alu0100783612

Tiempo invertido: **25** horas

Asignatura *Administración y diseño de Bases de Datos*
Grado en Ingeniería Informática,
1º Cuatrimestre

Universidad de La Laguna
Escuela Técnica Superior de Ingeniería Informática

Índice

1. Introducción.

La creciente importancia de la información en nuestra sociedad ha llegado incluso a convertirse en el principal activo de las empresas haciendo imprescindible su protección.
Esta protección abarca una gran cantidad de aspectos, como los siguientes:

- Seguridad física.
- Autenticación.
- Biometría.
- Seguridad en las redes de comunicación,
- Criptografía,
- Seguridad jurídica,
- etc.

Dentro de todos estos aspectos destaca, a nuestro juicio, la seguridad de las bases de datos, que es donde residen al fin y al cabo los datos a partir de los cuales las organizaciones obtienen la información y los conocimientos necesarios para su supervivencia.

La seguridad en las bases de datos ha sido ampliamente investigada desde hace varios años, pero debido a los continuos avances tecnológicos, los cada vez más complejos requisitos organizacionales, la difusión de las comunicaciones, el incremento de la vulnerabilidad de los sistemas de información, los cambios legislativos, etc., todavía constituye un problema que no se encuentra resuelto.

Además, en ningún caso se han aportado soluciones metodológicas en las que la seguridad sea considerada como un factor importante a lo largo del proceso de diseño de las bases de datos.

Basándonos en estos hechos, los campos de aplicación para la seguridad de las bases de datos son:

- Control de acceso
- Auditorias
- Autenticación
- Encriptación
- Control de integridad
- Copias de seguridad
- Seguridad de las aplicaciones.

2. Características.

Tenemos que tener cuidado y no confundir seguridad en las base de datos con bases de datos seguras.

Para que una base de datos se considere segura tiene que cumplir con ciertas características que la hacen segura.

Tales como:

- Vigilancia continua y controlada (monitoreo).
- Estrictos modos de acceso Lógicos.
- Cifrado de datos.
- Protección ataque cibernético (inyección de SQL).
- El bloqueo y la prevención, sin estar en línea para las transacciones.
- Descubrimiento activo de los datos en riesgo.
- Mejora de la visibilidad en el tráfico de aplicaciones.
- Firewall o Proxy de acceso.

Estas son las principales características que tienen las bases de datos seguros, no todas las bases de datos seguras tienen porque tener las mismas características. Pero estas son las más importantes.

3. Medidas de Seguridad

Las medidas de seguridad las podemos catalogar en dos grandes bloques, medidas físicas y mediadas lógicas.

Las medidas físicas se dividen también varios subgrupos tales como seguridad de acceso que se encargar de controlar quien accede físicamente a las bases de datos y que no se puedan pasar por alto las medidas de acceso y obligar a cumplirlas siempre, usando varias mediadas tales como tarjetas de control de acceso, control dactilar o llegando incluso a control de acceso con retina ocular.

Otro subgrupo de medidas físicas son las que combaten posibles catástrofes naturales tales como incendios, inundaciones, terremotos, etc.
Con medidas que van desde tener los datos de forma que siempre se puedan recuperar, medidas de extracción de oxígeno para apagar un incendio o suelo a distinto nivel para inundaciones, etc.

Las medidas de seguridad lógicas son más complejas que las físicas puesto que han de realizarse en las bases de datos de manera que se garantice la seguridad de la base de datos.

Para ello crearemos perfiles de usuarios en los que cada grupo de usuarios tiene distintos privilegios, con esto conseguimos que un usuario de una base de datos no pueda eliminar una tabla, etc.

Las vistas de las bases de datos son muy importantes puesto que delimitamos el contenido que se muestra de la base de datos a ciertos usuarios.

Una parte importante de la seguridad lógica de las bases de datos es la de permitir realizar auditorías a las bases de datos para ver qué datos contiene y de qué forma los contiene.

Finalmente dejamos la más importante de las medidas lógicas, la prevención de la inyección SQL, que básicamente consiste en modificar las consultas SQL que se realizan a la bases de datos para obtener información que no debería ser pública. Para evitar estas intrusiones aplicaremos 4 sencillos pasos:

- Asignación de privilegios mínimos: debe tener los privilegios necesarios.
- Validar los datos introducidos: especifique el tipo de dato de entrada, si son números, asegúrese de que son solo números.
- Utilizar procedimientos almacenados y aceptar los datos del usuario como parámetros en lugar de comandos SQL.
- Usar comillas dobles en lugar de simples.

4. Protocolos

Un **protocolo** es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red.

Existen diversos protocolos de acuerdo a cómo se espera que sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP), etc.

Un **protocolo de seguridad** es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica. Define las reglas que gobiernan estas comunicaciones. Diseñadas para que el sistema pueda soportar ataques de carácter maliciosos. Los protocolos son diseñados bajo ciertas primicias con respecto a los riesgos.

Los protocolos que se aplican a las bases de datos seguras dependen del proveedor SGBD y del lenguaje de programación que se quiera usar.

- Active Directory, término usado por Microsoft para referirse a su servicio de directorio en una red de computadores. Utiliza distintos protocolos tales como LDAP, DNS, DHCP, Kerberos, etc.

- SSL/TLS nivel seguro de socket o seguridad a nivel de trasporte, estándar IETF, utiliza certificados y socket TCP para proveer conexiones seguras.

Esta seguridad es en forma de privacidad y autenticación: por un lado autentica el servidor de la comunicación (mediante certificados), y por otra parte selecciona un algoritmo de cifrado, permite el intercambio de claves de forma segura entre cliente y servidor, y cifra la información con cifrado simétrico.

- Kerberos. Sistema de autentificación de única firma en red con posibilidad de privacidad. Estándar IETF, utiliza tecnología de clave simétrica.

- SSH (Secure Shell), protocolo de entrada en sesión y/o ejecución de comandos en una maquina remota.

- IKE (Internet Key Exchange), Protocolo utilizado para establecer una asociación de seguridad (SA) usando el protocolo IPsec, emplea un intercambio secreto de claves tipo Diffie-Hellman para establecer el secreto compartido de la sesión (suele usar sistemas de clave pública).

Algunos otros protocolos usados en las bases de datos NOsql.

- P2P con lo que la redundancia es máxima.

- Gossip para permitir comunicación dentro de un ring (cada nodo sabe de otros nodos), usado para descubrir la ubicación y la información de estado a cerca de los otros nodos.

5. Tipos de Base de Datos Seguras.

a. **DAM (Monitoreo de la actividad de base de datos)**: se refiere a un conjunto de herramientas que se pueden utilizar para apoyar la capacidad de identificar e informar sobre el comportamiento indeseable fraudulento, ilegal u otra, con un impacto mínimo en las operaciones del usuario y la productividad. Las herramientas, que han evolucionado desde el análisis básico de la actividad del usuario en y alrededor de los sistemas de gestión de bases de datos relacionales (RDBMS) que abarcan un conjunto más amplio de capacidades, como el descubrimiento y clasificación, gestión de vulnerabilidades, análisis de nivel de aplicación, prevención de intrusiones, el apoyo a seguridad estructurado de datos, integración de identidad y gestión de acceso y apoyo a la gestión de riesgos.

b. **DAS (Evaluación de seguridad de la base de datos)**: Es fundamentalmente un proceso que mide el riesgo de base de datos en un punto en el tiempo. El primer elemento de riesgo se mide mediante la evaluación de la susceptibilidad de una base de datos a una serie de vulnerabilidades conocidas y situaciones de ataque. Una vulnerabilidad podría ser un error de configuración del sistema de mejores prácticas, tales como la falta de una política de contraseñas de bases de datos; un error de codificación de software como un desbordamiento de búfer en un procedimiento; o un error de gestión de privilegios como el acceso público a una tabla sensible.

   Cada vulnerabilidad identificada es entonces clasificado por gravedad: bajo, medio, alto, crítico, etc. Finalmente, se genera un informe que resume los resultados. Un típico resumen de la evaluación, por ejemplo, el número total de vulnerabilidades por gravedad. Este resumen es esencialmente una instantánea global de gestión de riesgo que puede utilizar para priorizar los pasos necesarios para mejorar la seguridad de la base de datos.
   Indica a los administradores de seguridad de TI y administradores de bases de datos las bases de datos y las vulnerabilidades específicas que necesitan su atención primero.

c. **DBF (Firewalls de la base de datos)**: Los firewalls de la base de datos son un tipo de firewalls de aplicaciones Web que monitorean las bases de datos para identificar y proteger contra ataques específicos de base de datos que en su mayoría buscan para tener acceso a la información confidencial almacenada en las bases de datos. Los firewalls de la base de datos también permiten supervisar y auditar el acceso a las bases de datos a través de los registros mantenidos por ellos. Una base de datos Firewall puede generar informes de cumplimiento de normativas específicas, como PCI, SOX, etc.

   Los firewalls son dispositivos reforzados de seguridad/ software que se despliega bien en línea con el servidor de bases de datos (justo antes de que el servidor de base de datos) (OR) cerca de la puerta de enlace de red (cuando se trata de la protección de varias bases de datos en varios servidores). Algunos servidores de bases de datos admiten agentes basados en host que puede ser instalado en el servidor de bases de datos para supervisar los eventos de la base de datos local. Pero el hardware soporte de cortafuegos basados en host/network monitoring sin ninguna carga adicional en los servidores de bases de datos.

6. Ámbitos de Uso

Las bases de datos seguras se utilizan para aplicaciones, almacenar información, etc., donde existe un alto riesgo de sufrir ataques, perder información o modificarla inadecuadamente conlleva una alta inseguridad para los datos almacenados.

Ejemplos de Usos:

1. Bases de Datos Bancarias
   a. Datos de Cuentas Bancarias.
   b. Datos de los Clientes.
   c. etc.
2. Banca Online:
   a. PayPal.
   b. AliPay.
   c. Western Union.
   d. etc.
3. Comercio electrónico
   a. Ebay.

   b. AliExpress.
   c. AliBaba.
   d. etc.
4. Bases de datos Gubernamentales.
   a. Datos de antecedentes penales.
   b. Datos militares.
   c. Datos de la Hacienda Pública.
   d. etc.
5. Datos Hospitalarios.

Resumiendo todas las empresas públicas o privadas que requieran una base de datos donde se almacenen información de carácter privado o que ampare la LOPD.

7. Conclusión

Como resultado de la investigación y de la búsqueda de información de las Bases de Datos Seguras, hemos concluido que dichas bases de datos, se encargan de
Almacenar, gestionar u organiza los datos de carácter privado y que no deben ser perdidos modificados o robados bajo ningún concepto.

Aprendimos las características de seguridad que ofrecen estas bases de datos, que debido a los datos que almacenan las medidas de seguridad extraordinarias que son necesarias para intentar salvaguardar los ficheros de datos.

8. Actas.

El día 21 de Noviembre de 2015 quedamos decidir sobre los puntos de los que van a tratar nuestro trabajo, realizar el índice y el posible contenido del trabajo. Estábamos Borja Barrera Villagrasa alu0100498820 y Yeray Pérez Peraza alu0100783612.

El día 11 de diciembre de 2015 quedamos para terminar el trabajo corregir erratas, subir la documentación utilizada y realizar la presentación del trabajo. Estábamos Borja Barrera Villagrasa alu0100498820 y Yeray Pérez Peraza alu0100783612.

9. Bibliografía.

Referencias web:

https://en.wikipedia.org/wiki/Database_security. Octubre 2014

https://unidad-2-seguridad.wikispaces.com/2.4+Protocolos+de+seguridad.10 de Mayo de 2010

http://html.rincondelvago.com/seguridad-en-bases-de-datos.html. 1 febrero. 2001

DAM

https://en.wikipedia.org/wiki/Database_activity_monitoring. 3 Febrero 2009

DBF

http://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos. 16 de Julio de 2013

https://www.youtube.com/watch?v=h7K-VYeg75g. 10 de Mayo de 2012

http://www.muycomputerpro.com/2011/02/16/disponible-oracle-database-firewall-defensa-para-bases-de-datos. 16 de Febrero de 2011

DAS

Página.http://www.q-das.com/fileadmin/files2/manuals/esp/Q-DBM-Database_ESP_a.pdf. 15 de Mayo de 2014

https://www.oracle.com/database/security/index.html. 11 de Noviembre de 2016

https://docs.oracle.com/cd/B19306_01/server.102/b14220/security.htm. 4 de Enero de 2013.