TAREA 1 UNIDAD 1

Tomas Sebastián Hinojosa Meza.

Instituto Tecnológico de Pabellón de Arteaga.

Seguridad en Base de Datos

Profesor: Efrén Emmanuel Prado López

Tarea 1 U1.

Investigar los principales problemas de seguridad en bases de datos.

1. Gestión inadecuada de accesos

Las bases de datos deben estar protegidas y accesibles solo por usuarios autorizados, con inicios de sesión limitados. Firewalls pueden bloquear direcciones IP y las mismas restricciones deben aplicarse al sistema operativo y hipervisor. Estas restricciones pueden ralentizar el trabajo, pero son necesarias para proteger contra ataques.

2. Fácil acceso físico

Si los datos son almacenados de manera local en su centro de datos, siga las mismas reglas asegurándose de que solo la gente de confianza tenga acceso a la sala que contiene las unidades de disco físicas.

3. Copias de seguridad desprotegidas

Las copias de seguridad contienen la misma información, así que necesitan el mismo cuidado. Las cintas, unidades y otros medios estáticos deben guardarse en una caja fuerte.

4. Datos no cifrados en reposo

Los algoritmos para codificar datos suelen ser confiables porque han sido probados ampliamente y los estándares actuales no tienen debilidades conocidas públicamente. Ahora es fácil agregar un buen cifrado a la base de datos y las copias de seguridad para todos los datos en reposo. Incluso si los algoritmos y las implementaciones son seguros, las claves también deben protegerse cuidadosamente.

5. No utilizar algoritmos de protección de la privacidad

El cifrado es una buena herramienta para proteger copias físicas de la base de datos, siempre que se pueda resguardar la clave.

6. Falta de controles de proliferación

El objetivo de los arquitectos de almacenamiento de datos es minimizar el número de copias y garantizar que se destruyan en cuanto los datos no se utilicen. Si bien esto puede ser esencial para brindar un servicio estable, vale la pena pensar cuidadosamente sobre la proliferación durante el diseño. En algunos casos, puede ser posible limitar el copiado desenfrenado sin comprometer demasiado el servicio

7. Falta de controles de la base de datos

Asegurarse de que solo las aplicaciones correctas puedan ver las tablas adecuadas. No reutilizar la misma contraseña para todas las aplicaciones. No utilizar la que viene de forma predeterminada. Limite el acceso a los procesos locales o a la red local cuando sea posible.

8. Aplicaciones vulnerables con acceso a datos

La seguridad de la base de datos no vale mucho cuando una aplicación de confianza actúa de manera inadecuada. Un problema común es la inyección de SQL, Otro problema es la seguridad deficiente de la propia aplicación. En muchas arquitecturas, la aplicación lo ve todo. Si no se bloquean correctamente a los usuarios adecuados, todos los datos podrían verse comprometidos.

9. Exposición riesgosa a Internet

Es ideal que las bases de datos permanezcan en una parte de la red sin acceso público. Si la base de datos solo va a comunicarse con los servidores front-end, puede permanecer en una parte de la red donde únicamente estos servidores tengan acceso.

10. Falta de gestión de la integridad

La especificación de un esquema para los datos garantiza que los elementos de datos individuales se ajusten a un conjunto de reglas. El uso de transacciones y bloqueos evita que se introduzcan errores cuando una tabla o fila se actualiza y otra no.

Wayner, P. (2021, 10 enero). 12 fallas y errores de seguridad de las bases de datos (CIO Perú, Ed.). CIO Perú. https://cioperu.pe/articulo/33054/12-fallas-y-errores-de-seguridad-de-las-bases-de-datos/