EAE Business School

Píldora: Seguridad en las BBDD

Máster en Business Intelligence e Innovación Tecnológica

- La mayoría de bases de datos del mundo puede contener información sensible cuyo acceso inadecuado puede suponer un importante contratiempo.
- La principal medida es definir un conjunto de permisos correcto para los usuarios del sistema.
- Puede ser necesario almacenar cierta información de forma cifrada, especialmente por temas *LOPD*.
- Conocer los distintos ataques que podemos recibir puede servir para plantear unas medidas de seguridad efectivas.
- Otras contramedidas pueden ser, por ejemplo, la política de copias de seguridad.

Gestión de permisos

Al igual que en cualquier SO, se trata de la medida más básica a implementar y por ello la primera a afrontar.

Se trata simplemente de otorgar los permisos de accesos necesarios a los usuarios que vayan a consultar o modificar cada contenido, de forma que aquellos sin autorización no puedan realizar las tareas que no deberían.

Esta configuración se realiza gracias a las sentencias GRANT. Sintaxis:
GRANT [permiso] ON [nombre de bases de datos].[nombre de tabla] TO '[nombre de usuario]'@'localhost';

La sentencia inversa a GRANT sería REVOKE:
REVOKE [permiso] ON [nombre de base de datos].[nombre de tabla] FROM '[nombre de usuario]'@'localhost';

Para información más detallada consultar aquí.

Principales ataques

1.- Nombre de usuario/password en blanco, por defecto o débil.

No es nada raro conseguir en el día a día pares de usuario/password como sa/1234, esta el la primera línea de defensa y un punto fundamental de la armadura de nuestras bases de datos. Es importante hacer revisiones periódicas de credenciales.

2.- Inyecciones SQL.

Cuando la plataforma de base de datos falla para desinfectar las entradas, los atacantes son capaces de ejecutar las inyecciones SQL de forma similar a como lo hacen en los ataques basados en Web, lo que les permite elevar sus privilegios y obtener acceso a una amplia gama de funcionalidades. Muchos de los proveedores han dado a conocer soluciones para evitar estos problemas, pero no servirá de mucho si los parches no se aplican o no se toman los correctivos correspondientes.

Principales ataques

3.- Preferencia de privilegios de usuario por privilegios de grupo.

Las organizaciones necesitan garantizar que los privilegios no se les den a los usuarios por asignación directa quien finalmente los recogerá como conserjes recogen las llaves en sus llaveros. En cambio, Rothacker recomienda que los usuarios sólo reciban privilegios por parte de grupos o funciones y sean manejados colectivamente. De esta forma será más fácil eliminar derechos a un usuario con simplemente eliminarlo del grupo, sin que queden derechos ocultos u olvidados asignados a dicho usuario.

4.- Características de base de datos innecesariamente habilitadas.

Cada instalación de base de datos viene con paquetes adicionales de todas las formas y tamaños que en su mayoría rara vez son utilizados por una sola organización. Dado que el nombre del juego en materia de seguridad de base de datos es el de reducir las superficies de ataque, las empresas necesitan buscar los paquetes que no utilizan y desactivarlos. Esto no sólo reduce los riesgos de ataques (0) day a través de estos vectores, sino que también simplifica la gestión de parches.

Principales ataques

5.- Configuración de seguridad ineficiente.

Del mismo modo, las bases de datos tienen una gran cantidad opciones de configuración y consideraciones diferentes a disposición de los administradores para ajustar el rendimiento y funcionalidades mejoradas. Las organizaciones necesitan conseguir y desactivar aquellas configuraciones inseguras que podrían estar activadas por defecto para mayor comodidad de los DBA o desarrolladores de aplicaciones. Las configuraciones de bases de datos en producción y desarrollo deben ser radicalmente diferentes.

6.- Desbordamientos de búfer.

Otro favorito de los piratas cibernéticos, las vulnerabilidades de desbordamiento de búfer, son explotadas por las inundaciones de las fuentes de entrada con valores diferentes o muy superiores a los que aplicación espera - por ejemplo, mediante la adición de 100 caracteres en un cuadro de entrada pidiendo un número de Seguro Social. Los proveedores de bases de datos han trabajado duro para solucionar los problemas técnicos que permiten estos ataques se produzcan. Esta es otra razón por la cual los parches son tan importantes.

Principales ataques

7.- Escalada de privilegios

Del mismo modo, las bases de datos con frecuencia exponen vulnerabilidades comunes que permiten a un atacante escalar privilegios en una cuenta de privilegios bajos hasta tener acceso a los derechos de un administrador. A medida que estas vulnerabilidades son descubiertas, los proveedores las corrigen y los administradores deben mantener las actualizaciones y parches actualizados.

8.- Ataque de denegación de servicio

El caso del SQL Slammer es siempre un ejemplo muy esclarecedor de cómo los atacantes pueden utilizar las vulnerabilidades de los DBMS para derribar los servidores de base de datos a través de un alto flujo de tráfico. Aún más ilustrativo es el hecho de que cuando el Slammer atacó en 2003, un parche ya estaba por ahí que se dirigió a corregir la vulnerabilidad por la que se generó su ataque. Hoy en día siete años más tarde, SQL Slammer todavía está dando dolores de cabeza en los servidores no actualizados.

Principales ataques

9.- Bases de datos sin actualizar.

Esto podría sonar repetitivo, pero vale la pena repetirlo. Los administradores de base de datos a veces no aplican un parche en el momento oportuno porque tienen miedo de este dañe sus bases de datos. Pero el riesgo de ser hackeado hoy es mucho más alto que el riesgo de aplicar un parche que descomponga la base de datos. Además exixten ante esos temores los backups y las réplicas. Quizás este punto pudo haber sido válido hace cinco años, pero los proveedores ahora
Sin encriptar los datos sensibles en reposo y en movimiento

10.- Datos sensibles sin cifrar, tanto en reposo como en movimiento.

Tal vez sea una obviedad, pero las organizaciones no deben almacenar los datos sensibles en texto plano en una tabla. Y todas las conexiones a la base de datos siempre que manejen datos sensibles deben utilizar el cifrado.

Principales ataques

11.- Exposición de datos en copia de seguridad.

Es bastante frecuente encontrar sistemas con un grado de securización maduro que, por temas de presupuesto, gestionan sus copias de seguridad desde otros mucho más débiles. Hay que tener en cuenta que pese a no ser un sistema productivo, una máquina de backup contendrá toda la información de la base de datos por lo que ésta estará potencialmente expuesta.

12.- Ataques de sniffing.

Los ataques de sniffing son aquellos que, desde aplicaciones de “escucha”, interceptan las comunicaciones. Un protocolo de autenticación mal implementado, un envío de credenciales por canales no seguro u otras irregularidades similares podrían verse sujetas a ser interceptadas y con ello, la información que comunican.