Unidad # 2
Seguridad de los Datos

Administración de Bases de Datos II

Gisela Yasmín García Espinoza

Competencia de la asignatura

Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje No SQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.

Contenidos a desarrollar

- ¿Qué es la seguridad de la base de datos?
- Desafíos
- Riesgos para una base de datos
- Prácticas de seguridad recomendadas

Seguridad en las bases de datos en entornos web

¿Qué es la seguridad de la base de datos?

La seguridad de la base de datos se refiere a las diversas medidas que toman las organizaciones para garantizar que sus bases de datos estén protegidas de amenazas internas y externas. La seguridad de la base de datos incluye proteger la propia base de datos, los datos que contiene, su sistema de administración de bases de datos y las diversas aplicaciones que acceden a ella. Las organizaciones deben proteger las bases de datos de ataques deliberados, como amenazas a la seguridad cibernética, así como del uso indebido de datos y bases de datos por parte de quienes pueden acceder a ellos.

Desafíos de seguridad

Las preocupaciones por la seguridad de los ataques basados en Internet son algunos de los desafíos más persistentes para la seguridad de las bases de datos. Los piratas informáticos idean nuevas formas de infiltrarse en las bases de datos y robar datos casi a diario. Las organizaciones deben asegurarse de que las medidas de seguridad de sus bases de datos sean lo suficientemente sólidas para resistir estos ataques. Algunas de estas amenazas de seguridad cibernética pueden ser difíciles de detectar, como las estafas de phishing en las que las credenciales del usuario se ven comprometidas y se utilizan sin permiso. El malware y el ransomware también son amenazas comunes a la seguridad cibernética.

Otro desafío crítico para la seguridad de la base de datos es asegurarse de que los empleados, socios y contratistas con acceso a la base de datos no abusen de sus credenciales.

Riesgos para una base de datos

Denegación de servicio (DoS): el búfer se desborda debido a problemas de DoS. Esta es una amenaza común para sus datos. También puede deberse a la corrupción de datos y, cuando se produce un ataque de este tipo, el servidor se bloquea y no puede acceder a los datos. Su sitio web permanecerá inactivo, lo que provocará la pérdida de negocios y una mala reputación.

Escalada de privilegios: esta es una de las amenazas más graves para su base de datos porque puede causar un caos total en su negocio. Este problema hace que su base de datos sea propensa a la pérdida de datos, la adición malintencionada de datos y la modificación.

Riesgos para una base de datos

Desbordamiento de búfer: esta es la amenaza de seguridad de base de datos más común. Un programa puede precipitar esto al intentar copiar demasiados datos en un búfer, lo que provoca un desbordamiento. Esto puede provocar que se sobrescriban los datos que ya están en la memoria. Si un ataque ocurre en ese momento, causará estragos en su sitio web.

Inyecciones SQL: esta es, con mucho, la mayor amenaza para su base de datos. Estos son un riesgo tanto para las aplicaciones web como para las bases de datos. El problema ocurre cuando los datos que no han sido desinfectados llegan a la base de datos. Un pirata informático puede acceder a información confidencial. Esto puede arruinar tu negocio.

Como implementar seguridad?

Hay tres capas de seguridad de la base de datos: el nivel de la base de datos, el nivel de acceso y el nivel del perímetro. La seguridad a nivel de la base de datos se produce dentro de la propia base de datos, donde viven los datos. La seguridad de la capa de acceso se centra en controlar quién puede acceder a ciertos datos o sistemas que los contienen. La seguridad de la base de datos a nivel del perímetro determina quién puede y quién no puede ingresar a las bases de datos. Cada nivel requiere soluciones de seguridad únicas.

Como implementar seguridad?

Nivel de seguridad	Soluciones de seguridad
Nivel de base de datos	• Enmascaramiento • Tokens • Cifrado
Nivel de acceso	• Listas de control de acceso • Permisos
Nivel perimetral	• Cortafuegos • Redes privadas virtuales

Prácticas de seguridad recomendadas

Garantizar la seguridad de la base de datos física

En el sentido tradicional, esto significa mantener el servidor de base de datos en un entorno seguro y bloqueado con controles de acceso para mantener fuera a las personas no autorizadas. Pero también significa mantener la base de datos en una máquina física separada, eliminada de las máquinas que ejecutan aplicaciones o servidores web.

Prácticas de seguridad recomendadas

Monitoreo de la actividad de la base de datos

Este es uno de los componentes más importantes a la hora de proteger una base de datos. Los servicios de DBA utilizan esta consideración al proteger su sistema.

El DAM es crucial, ya que monitorea todo lo que sucede en la base de datos y envía alertas sobre cualquier cosa sospechosa. Sabrá quién está accediendo a la base de datos y a qué hora. Un sistema de informes completo es fundamental para proteger la base de datos contra piratas informáticos y otras intrusiones.

Prácticas de seguridad recomendadas

Aplicaciones y Firewall

El uso de aplicaciones web y firewalls es una de las mejores prácticas de seguridad de bases de datos en la capa perimetral. Los cortafuegos evitan que los intrusos accedan a la red de TI de una organización a través de Internet; son un requisito previo crucial para las preocupaciones de seguridad cibernética. Las aplicaciones web que interactúan con bases de datos pueden protegerse mediante software de gestión de acceso a aplicaciones. Esta medida de seguridad de la base de datos es similar a las listas de control de acceso y determina quién puede acceder a las aplicaciones web y cómo pueden hacerlo. También hay firewalls para aplicaciones web individuales que brindan los mismos beneficios que los firewalls tradicionales.

Prácticas de seguridad recomendadas

Cifrado

El cifrado es una de las prácticas de seguridad de bases de datos más efectivas porque se implementa donde están los datos en la base de datos. Sin embargo, las organizaciones pueden cifrar los datos en movimiento y en reposo, de modo que estén protegidos mientras fluyen entre los sistemas de TI de una organización. Los datos cifrados se transfiguran, por lo que aparecen de forma difícil de comprender a menos que se descifren con las claves adecuadas. Por lo tanto, incluso si alguien puede acceder a datos cifrados, no tendrá sentido para ellos. El cifrado de la base de datos también es clave para mantener la privacidad de los datos y puede ser eficaz para la seguridad de IoT .

Prácticas de seguridad recomendadas

Acceso a la base de datos

La administración de contraseñas y permisos es fundamental para mantener la seguridad de la base de datos. Esta tarea suele estar supervisada por empleados de seguridad dedicados o equipos de TI.

En algunos casos, esta práctica recomendada de seguridad de la base de datos implica listas de control de acceso. Las organizaciones pueden tomar muchos pasos diferentes para administrar las contraseñas, como el uso de medidas de autenticación de factores duales o múltiples, o dar a los usuarios una cantidad limitada de tiempo para ingresar las credenciales. Sin embargo, esta práctica requiere una actualización constante de las listas de acceso y permisos. Puede llevar mucho tiempo, pero los resultados lo valen.

Prácticas de seguridad recomendadas

Aislar bases de datos confidenciales.

Es muy difícil penetrar en la seguridad de las bases de datos si las bases de datos confidenciales están aisladas. Dependiendo de cómo se implementen las técnicas de aislamiento, es posible que los usuarios no autorizados ni siquiera sepan que existen bases de datos confidenciales. Los perímetros definidos por software son un medio útil para aislar bases de datos confidenciales para que no parezcan estar en la red de un usuario en particular.

Este enfoque dificulta la toma de bases de datos con ataques de movimiento lateral ; también es eficaz contra ataques de día cero . Las estrategias de aislamiento son una de las mejores formas de solidificar la seguridad de la base de datos a nivel de acceso. Las soluciones de aislamiento competitivas combinan este enfoque con la seguridad de la capa de la base de datos, como las claves públicas y el cifrado.

Prácticas de seguridad recomendadas

Cambios

La gestión de cambios requiere describir, idealmente con anticipación, qué procedimientos deben realizarse para proteger las bases de datos durante el cambio. Los ejemplos de cambios incluyen fusiones, adquisiciones o simplemente diferentes usuarios que obtienen acceso a varios recursos de TI.

Es necesario documentar qué cambios se llevarán a cabo para el acceso seguro a las bases de datos y sus aplicaciones. También es importante identificar todas las aplicaciones y sistemas de TI que utilizarán esa base de datos, además de sus flujos de datos..

Prácticas de seguridad recomendadas

Auditoría

Esto incluye supervisar los inicios de sesión (e intentos de inicio de sesión) en el sistema operativo y la base de datos y revisar los registros con regularidad para detectar actividad anómala.

La supervisión eficaz debería permitir detectar cuándo una cuenta se ha visto comprometida, cuándo un empleado está realizando actividades sospechosas o cuándo la base de datos está siendo atacada. También debería ayudar a determinar si los usuarios están compartiendo cuentas y enviar alertas si las cuentas se crean sin permiso (por ejemplo, por un pirata informático).

Tabla de actividades	
Nombre de la actividad	Seguridad Web en Bases de Datos
Tipo de actividad	Investigación bibliográfica
Tipo de participación	Individual
Competencias especifica de la asignatura	Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje No SQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.
Instrucciones	Después de haber dado lectura a los contenidos de la semana, desarrolle un ejemplo práctico en donde haga uso de una práctica de seguridad para base de datos en la web, deberá presentar el resultado el día de la clase
Fecha de entrega	Durante desarrollo de clase
Instrumento de evaluación	Rúbrica
Ponderación	Formativa

Recursos Complementarios		
Recurso	Título	Cita Referencial
Sitio Web	Seguridad de la base de datos	https://www.akamai.com/es/es/resources/database-security.jsp
Documento pdf	Seguridad en Bases de Datos y aplicaciones Web	http://openaccess.uoc.edu/webapps/o2/bitstream/10609/62886/4/Seguridad%20en%20bases%20de%20datos_M%C3%B3dulo%201_Introducci%C3%B3n.pdf

¿Preguntas?

¡Muchas gracias!

UNIVERSIDAD GERARDO BARRIOS
Líderes en Gestión del Conocimiento

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2019- 2024