Estrategias de seguridad en base de datos

Laura Atencio Nilson Felix, Velasco Sucapuca, Andree

Resumen

Cuando hablamos de integridad en base de datos nos estamos refiriendo a la completitud, la exactitud y la coherencia del conjunto de datos de una base de datos. Podemos tener una percepción de esta **integridad en base de datos** cuando vemos que entre dos instancias o entre dos actualizaciones de un registro de datos, no hay ninguna alteración, lo que significa que los datos están intactos y sin cambios..

Palabras clave: Seguridad, actualizaciones, instancia.

Abstract

When we speak of integrity based on the data, we are referring to the integrity, the accuracy and the coherence of the data set of a database. We can have a perception of this integrity in the database when we see that between two instances or updates of a data record, there is no alteration, which means that the data is intact and unchanged.

Keywords: Security, updates, instance..

I. INTRODUCCIÓN

La seguridad de la información se ocupa de proteger la confidencialidad, disponibilidad e integridad en base de datos de todos los activos de conocimiento de la organización. La forma de lograrlo tiene que ver con:

- **Confidencialidad**: se trata del aspecto más importante de la seguridad de base de datos. Este objetivo se alcanza a través del La encriptación ha de aplicarse a datos en reposo, pero también a los datos que, por un motivo u otro, se encuentren en tránsito.

- **Integridad en base de datos**: **busca garantizar que sólo las personas autorizadas a ello podrán acceder a información privilegiada de la empresa**. La integridad de una base de datos se aplica a través de protocolos de autenticación, políticas internas (como las que impulsan la seguridad de las contraseñas) y un sistema de control de acceso de usuario que define los permisos que determinan quién puede acceder a qué datos. Tampoco puede olvidarse el tomar medidas que ayuden a **conseguir que las cuentas no utilizadas queden bloqueadas o sean eliminadas.**

- **Disponibilidad:** hace referencia a la necesidad de que las bases de datos y toda la información que contienen estén listas para su uso. Por una parte, se **debe garantizar su funcionalidad y confiabilidad** mientras que, por otra, es recomendable planificar los tiempos de inactividad fuera del horario laboral.

Garantizar la **integridad en base de datos**, así como su disponibilidad y confiabilidad es determinante para el buen funcionamiento del negocio. Sin embargo, la amenaza no da tregua y, a día de hoy, los ataques se multiplican, tanto en frecuencia, como en objetivo. **Los piratas informáticos ya no codician sólo los activos informacionales de las grandes corporaciones multinacionales, sino que tienen en su punto de mira a todo tipo de empresas,**independientemente de su tamaño, propósito o industria.

II. OBJETIVOS

- **Recurrir al enmascaramiento de datos** o permitir a los usuarios acceder a cierta información sin poder verla ayuda a mantener la confidencialidad incluso en entornos de pruebas.

- **Minimizar los extras y limitarse a los servicios, aplicaciones y funcionalidades que realmente son necesarios**para asegurar el normal funcionamiento de las operaciones del negocio, de esta forma se reduce el riesgo.

- **Asegurarse de que los administradores de la base de datos entiendan la importancia de garantizar su protección.**

- **Mantener actualizadas las bases de datos** y eliminar los componentes desconocidos.

- **Recurrir a herramientas como el análisis de código estático**, que ayudan a reducir los problemas de inyección de SQL, desbordamiento de búfer y problemas de configuración.

- **Hacer copias de seguridad frecuentes** y emplear una fuente de alimentación ininterrumpida o SAI que garantice que un corte de energía no causa la pérdida de datos.

III. MARCO TEÓRICO

A. ¿Qué es seguridad de base de datos?

La seguridad de la información se ocupa de proteger la confidencialidad, disponibilidad e integridad en base de datos de todos los activos de conocimiento de la organización. La forma de lograrlo tiene que ver con:

- **Confidencialidad**: se trata del aspecto más importante de la seguridad de base de datos. Este objetivo se alcanza a través del La encriptación ha de aplicarse a datos en reposo, pero también a los datos que, por un motivo u otro, se encuentren en tránsito.

- **Integridad en base de datos**: **busca garantizar que sólo las personas autorizadas a ello podrán acceder a información privilegiada de la empresa**. La integridad de una base de datos se aplica a través de protocolos de autenticación, políticas internas (como las que impulsan la seguridad de las contraseñas) y un sistema de control de acceso de usuario que define los permisos que determinan quién puede acceder a qué datos. Tampoco puede olvidarse el tomar medidas que ayuden a **conseguir que las cuentas no utilizadas queden bloqueadas o sean eliminadas.**

- **Disponibilidad:** hace referencia a la necesidad de que las bases de datos y toda la información que contienen estén listas para su uso. Por una parte, se **debe garantizar su funcionalidad y confiabilidad** mientras que, por otra, es recomendable planificar los tiempos de inactividad fuera del horario laboral.

Garantizar la **integridad en base de datos**, así como su disponibilidad y confiabilidad es determinante para el buen funcionamiento del negocio. Sin embargo, la amenaza no da tregua y, a día de hoy, los ataques se multiplican, tanto en frecuencia, como en objetivo. **Los piratas informáticos ya no codician sólo los activos informacionales de las grandes corporaciones multinacionales, sino que tienen en su punto de mira a todo tipo de empresas,**independientemente de su tamaño, propósito o industria.

Tipos de ataques a la integridad en base de datos

Está claro **que el riesgo implícito en este tipo de acciones maliciosas varía de una organización a otra**, aunque entre los ataques más comunes se encuentran los que tienen como objetivo:

- **Datos personales de clientes, números de tarjetas de crédito y seguridad social.**
- **Detalles estratégicos del negocio.**
- **Información financiera de la propia compañía y de sus socios.**
- **Datos sensibles acerca de los empleados.**

Podría decirse que se trata de la mayoría de las bases de datos activas en los directorios de la empresa, al menos, todas las que, de alguna forma, resultan relevantes para el negocio. Precisamente por ello, es necesario mantener sólidas prácticas de seguridad y **estrategias de defensa que permitan combatir este tipo de ataques, también en sus versiones más recientes y sofisticadas, como el phisinig, el spear phising, la inyección SQL, el DDos, la amenaza persistente avanzada o el ransomware.**

Según la Encuesta de Amenazas de Inyección SQL de Ponemon, "*el 65% de las organizaciones encuestadas habían experimentado un exitoso ataque de estas características en el último año*". Entre las **causas que podrían haber motivado la vulneración de la integridad en base de datos se encuentran la falta de escaneo de database o su escaneo irregular, un error común en el 47% de los casos.**

Se trata de un dato sorprendente, sobre todo si se tiene en cuenta que, el 49% de los encuestados calificaron el nivel de amenaza de una inyección de SQL en su organización con una puntuación de 9 o 10.

Sin embargo, no hace falta ir tan lejos**, la autenticación débil es la amenaza más común a la seguridad y la integridad en base de datos**. Una misma contraseña usada con fines distintos, compartida entre usuarios, que nunca se actualiza o que resulta obvia facilita el trabajo de un atacante malintencionado en su misión encaminada a **robar la identidad de un usuario** legítimo. Una vez que conoce esos 8, 10 o 12 dígitos, ya tiene acceso a datos confidenciales, ya tiene a la organización en sus manos.

B. Principios básicos de la seguridad de base de datos

Uso de contraseñas seguras

Al pensar en mecanismos que contribuyan a la seguridad de los datos, es muy importante **utilizar contraseñas robustas**, capaces de **resistir ataques informáticos**. Un software para descubrir contraseñas de forma automatizada es capaz de probar millones de combinaciones en minutos, por lo que no debe subestimarse la función que juega una buena contraseña en proteger nuestros datos.

Algunas claves para crear contraseñas seguras:

- **Crear contraseñas largas**. Algunos sistemas solicitan un mínimo de 7 u 8 caracteres. Para mayor seguridad, pueden utilizarse 15 caracteres o más, especialmente para proteger aquellos servicios que se consideran críticos
- **Utilizar mayúsculas, minúsculas, signos de puntuación y caracteres no alfabéticos**
- **Utilizar contraseñas únicas para cada servicio**. Por ejemplo, no utilizar una misma clave para proteger datos almacenados en un servidor institucional y en un servicio de almacenamiento en la nube.
- **Evitar errores comunes**, tales como:
    - Utilizar palabras de diccionario, aún si están en otros idiomas
    - Utilizar datos personales, tales como números de identificación, teléfonos o direcciones
    - Utilizar referencias a la cultura popular, tales como nombres de libros, personajes, canciones, bandas musicales, etc.
- Puede utilizarse el **enfoque XKCD**, que consiste en utilizar cuatro palabras escogidas al azar. Para fortalecer la contraseña, sustituir algunas de las letras por signos y números, utilizando mayúsculas y minúsculas.
- Otro enfoque es **utilizar un gestor de contraseñas**, software que genera y maneja contraseñas únicas y encriptadas, ofreciendo mayores garantías de seguridad y evitando el problema de crear y recordar múltiples contraseñas

Y por supuesto, deben tomarse las precauciones que se recomiendan para la protección de cualquier contraseña, como **evitar ingresar a cuentas desde conexiones públicas o en espacios inseguros**.

Encriptación

La **encriptación** es el proceso que permite **convertir datos a una forma o código no reconocible o legible**. El uso de la encriptación permite **proteger datos que son importantes o sensibles**, previniendo que otros tengan acceso a ellos. Para que esto sea así, luego de ser encriptados, se debe utilizar una contraseña para tener acceso a los datos en su forma original.

La encriptación **puede utilizarse a diferentes niveles**, desde un archivo único a una carpeta o un volumen mayor de información, incluso un dispositivo como un disco USB, teléfono móvil o una laptop. También pueden encriptarse los datos que serán transmitidos a través de una red. De esta manera, **el encriptado da mayor seguridad a los datos en caso de haber una pérdida no intencionada o un ataque virtual o físico a los medios donde se almacenan**.

Al encriptar datos, debe tenerse en cuenta que:

- La encriptación no substituye otros métodos de protección de la información
- La encriptación depende del uso de contraseñas seguras
- Cuando se pierde la contraseña o cuando los dispositivos se dañan, los datos encriptados se perderán

Por esto, **es importante que la encriptación se utilice junto con otros métodos para garantizar la seguridad de los datos**, y que estos cuenten con un **respaldo apropiado**.

Otras medidas de seguridad

Otros mecanismos de defensa ante ataques que debe considerarse es el u**so y actualización constante de antivirus** en todas las estaciones desde las cuales se esté realizando el trabajo de investigación.

Este tipo de medidas es especialmente importante cuando se trabaja con **datos sensibles o confidenciales**. En estos casos, es ideal que el almacenamiento se haga en **dispositivos no conectados a redes**, y en

caso de ser imposible, **encriptar todos los datos almacenados**, especialmente aquellos que serán transmitidos.

Por último, debe recordarse que la seguridad no depende solo de la protección ante ataques informáticos. La **seguridad física** es igualmente importante, y pasa por medidas tales como almacenar los datos en dispositivos que se encuentren en **espacios bien protegidos**, lo que podría evitar el robo y/o daño a la información. En estos casos, el **mantenimiento de respaldos actualizados** es también de vital importancia.

1. PRIVILEGIOS EXCESIVOS

Cuando a un usuario se le entregan privilegios de la base de datos que excedan los requerimientos de su puesto de trabajo, el riesgo que se crea puede ser innecesario.

La solución a este problema (además de buenas políticas de contratación) es el control de acceso a nivel de consulta. El control de acceso a nivel de consulta restringe los privilegios de las operaciones a solo utilizar los datos mínimos requeridos. La mayoría de las plataformas de seguridad de bases de datos nativas ofrecen algunas de estas capacidades (triggers, RLS, y así sucesivamente), pero el diseño de estas herramientas manuales las hacen impracticables en todo excepto en las implementaciones más limitados según experiencia de expertos de seguridad web.

2. ABUSO DE PRIVILEGIOS

Muchos de los usuarios pueden llegara a abusar de los privilegios de acceso de datos legítimos para fines no autorizados. Por ejemplo: suministrar información confidencial de un cliente, sustraer información de la compañía para su propio lucro.

La estrategia para lograr esta solución esta relacionada con la política de control de acceso que se aplican no sólo a lo que los datos son accesibles, pero ¿cómo se accede a los datos? Al hacer cumplir las políticas de seguridad web, sobre cosas como la ubicación, el tiempo, el cliente de aplicación y el volumen de los datos recuperados, es posible identificar a los usuarios que están abusando de los privilegios de acceso.

3. ELEVACIÓN DE PRIVILEGIOS NO AUTORIZADOS

Los atacantes pueden aprovechar las vulnerabilidades en el software de gestión en la base de datos para convertir los privilegios de acceso de bajo nivel de privilegios de acceso de alto nivel. Por ejemplo, sin seguridad de bases de datos, un atacante podría aprovechar una vulnerabilidad de desbordamiento de búfer de base de datos para obtener privilegios administrativos.

Exploits de elevación de privilegios pueden ser derrotados con una combinación de control de acceso a nivel de consulta, auditoría de base de datos y los sistemas de prevención de intrusiones (IPS) tradicionales. Control de acceso a nivel de consulta puede detectar un usuario que de repente utiliza una operación de SQL inusual, mientras que un IPS puede identificar una amenaza específica de seguridad web documentada dentro de la operación.

4. VULNERABILIDADES DE LA PLATAFORMA

Las vulnerabilidades en los sistemas operativos pueden conducir al acceso no autorizado a datos y la corrupción.

Las herramientas de IPS son una buena manera de identificar y / o bloquear ataques diseñados para aprovechar las vulnerabilidades de la plataforma de base de datos.

5. INYECCIÓN DE SQL

La mayoría de las aplicaciones web desarrolladas hoy en día hacen **uso de una base de datos para ofrecer páginas dinámicas y almacenar información tanto de los usuarios como de la propia herramienta, el uso de este tipo de lenguaje ha traido consigo la aparición de numerosas vulnerabilidades. Los Ataques de inyección SQL implican a un usuario que se aprovecha de vulnerabilidades en aplicaciones web y procedimientos almacenados para proceder a enviar consultas de bases de datos no autorizadas, a menudo con privilegios elevados.**

Soluciones de seguridad de bases de datos, auditoría de base de datos, control de acceso a nivel de consulta detecta consultas no autorizadas inyectadas a través de aplicaciones web y / o procedimientos almacenados.

6. AUDITORÍA DÉBIL

En los últimos años, las redes empresariales han evolucionado considerablemente. Todo, desde el computo móvil hasta la nube, todos los sistemas están haciendo que las redes actuales sean más complejas que nunca, incluso las mismas herramientas que son utilizadas para administrar la seguridad de red pueden expandir el ataque y crear vulnerabilidades. Las políticas débiles de auditoría de base de datos representan riesgos en términos de cumplimiento, la disuasión, detección, análisis forense y recuperación.

Por desgracia, el sistema de gestión de base de datos nativa (DBMS) audita las capacidades que dan lugar a una degradación del rendimiento inaceptable y son vulnerables a los ataques relacionados con el privilegio– es decir, los desarrolladores o administradores de bases (DBA) puede desactivar la auditoría de base de datos.

La mayoría de las soluciones de auditoría de base de datos también carecen del detalle necesario. Por ejemplo, los productos DBMS rara vez se registran qué aplicación se utiliza para acceder a la base de datos, las direcciones IP de origen y falló de consultas.

Las soluciones de auditoría de base de datos basados en la red son una buena opción. Tales soluciones de auditoría de base de datos no deben tener ningún impacto en el rendimiento de base de datos, operan de forma independiente de todos los usuarios y ofrecen la recopilación de datos a detalle.

7. DENEGACIÓN DE SERVICIO

En internet, un ataque de denegación de servicios (DDOS) es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando La denegación de servicio (DoS, aunque puede ser invocadas muchas técnicas. Las técnicas más comunes de DOS incluyen desbordamientos de búfer, corrupción de datos, la inundación de la red y el consumo de recursos.

La prevención de DoS debería ocurrir en múltiples capas que incluyendo los de red, aplicaciones y bases de datos según recomendaciones de cursos de seguridad de bases de datos y seguridad web.

Recomendaciones sobre las bases de datos incluyen el despliegue de un IPS y controles de la velocidad de conexión. Al abrir rápidamente un gran número de conexiones, los controles de velocidad de conexión pueden impedir que los usuarios individuales usan los recursos del servidor de base de datos.

8. VULNERABILIDADES EN LOS PROTOCOLOS DE LAS BASES DE DATOS

Existe una constante preocupación por la seguridad de la base de datos: Muchas veces la seguridad se ve afectada por la configuración de los procesos de conexión. Las vulnerabilidades en los protocolos de bases de datos pueden permitir el acceso no autorizado a datos, la corrupción o la disponibilidad. Por ejemplo, SQL Slammer worm se aprovechó de una vulnerabilidad de protocolo de Microsoft SQL Server para ejecutar código de ataque en los servidores de base de datos destino.

Los protocolos de ataques pueden ser derrotados mediante el análisis y validación de las comunicaciones de SQL para asegurarse de que no están malformados. Pueden aprender más sobre este ataque durante cursos de seguridad suministrados por Ona Systems,

9. AUTENTICACIÓN DÉBIL

La autenticación basada en contraseña es probablemente una de las funciones más importantes que se usan todos los días, sin embargo no se ha evolucionado mucho desde los primeros sistemas informáticos de

usuarios múltiples, incluso cuando se desarrollan métodos más seguros. Los esquemas de autenticación débiles permiten a los atacantes asumir la identidad de los usuarios de bases de datos legítimos. Estrategias de ataque específicas incluyen ataques de fuerza bruta, la ingeniería social, y así sucesivamente.
La implementación de contraseñas o autenticación de dos factores es una necesidad. Para la escalabilidad y facilidad de uso, los mecanismos de autenticación deben integrarse con las infraestructuras del directorio / gestión de usuarios de la empresa y seguridad web.

10. LA EXPOSICIÓN DE LOS DATOS DE BACKUP

El robo de información y la filtración de datos confidenciales son noticias del día a día, Algunos ataques recientes de alto perfil han involucrado el robo de cintas de backup de base de datos y discos duros.
Es importante que todas las copias de seguridad deben ser cifradas. De hecho, algunos proveedores han sugerido que los futuros productos DBMS no deberían admitir la creación de copias de seguridad sin cifrar. El cifrado de base de datos en línea es un pobre sustituto de controles granulares de privilegios acuerdo a expertos de seguridad de base de datos.

IV. CONCLUSIONES

Aunque muchas de las bases de datos y sus contenidos puedes ser vulnerables a muchas series de amenazas internas y externas, es posible reducir muchos de los ataques hasta casi a cero con ayuda de las soluciones y estrategias de seguridad sumnistradas por Ona Systems.

[1] A. Anonimo. Caracter´ısticas de la base de datos. urlhttp://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/11-caractersticas-de-la-base-de-datos.html, 2015.

[2] E. Chicano Tejada. *Utilización de los bases de datos relacionales en el sistema de gestión y almacenamiento de datos*. 2016.

[3] J. Lopez and A. Zuluaga. Metodología para el control de riesgos para la auditor´ıa de bases de datos. urlhttp://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4153/0 2013.

[4] oracle. *La importancia de establecer una política de seguridad para su base de datos*. 2019.

[5] C. Vergara. Ataque a la base de datos. urlhttp://ataquebd.blogspot.com/, 2012.