Estrategias de seguridad en base de datos*

Universidad Privada de Tacna

Juan Rodriguez Mamani†
Universidad Privada de Tacna
Tacna, Perú
nyxjuan@hotmail.com

ABSTRACT

Las bases de datos, por definición, contienen datos, y datos como la información de la tarjeta de crédito son valiosos para los delincuentes. Eso significa que las bases de datos son un objetivo atractivo para los piratas informáticos, y es por eso que la seguridad de la base de datos es de vital importancia.

Databases - by definition - contain data, and data such as credit card information is valuable to criminals. That means databases are an attractive target to hackers, and it's why database security is vitally important.

ACM Reference format:
Juan Rodriguez Mamani. 2018. Estrategias de seguridad en base de datos. In *Proceedings of Estrategias de seguridad en base de datos, Tacna - Perú, Diciembre 2018 (UNIVERSIDAD PRIVADA DE TACNA),* 4 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCCIÓN

La seguridad de datos es un tema de suma importancia que nos afecta a casi todos nosotros. Cada vez son más los productos tecnológicos que de una u otra forma deben ser tenidos en cuenta para temas de seguridad y que se están introduciendo en nuestra vida cotidiana, desde smartwatches hasta vehículos sin conductor. Ya ha llegado la era del Internet de las Cosas (IoT) y, por supuesto, de los hacks relacionados con IoT. Todos estos dispositivos conectados crean nuevas "conversaciones" entre dispositivos, interfaces, infraestructuras privadas y la nube, lo que a su vez crea más oportunidades para que los hackers puedan escuchar. Todo esto ha impulsado una demanda de soluciones y expertos en seguridad de datos que sean capaces de construir redes más fuertes y menos vulnerables.

Tendencias recientes han demostrado que los ataques de ransomware están aumentando en frecuencia y en gravedad. Se ha convertido en un negocio en auge para ladrones cibernéticos y hackers, que acceden a la red y secuestran datos y sistemas. En los últimos meses, grandes empresas y otras organizaciones, así como también usuarios particulares, han caído víctimas de este tipo de ataques y han tenido que pagar el rescate o correr el riesgo de perder datos importantes.

2 OBJETIVOS

Comprender la importancia de las estrategias de Seguridad de la Base de Datos

3 MARCO TEÓRICO

El término de bases de datos fue escuchado por primera vez en 1963, en un simposio celebrado en California, USA. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada ó estructurada.

3.1 Definición de Base de Datos

Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

3.2 Características

Entre las principales características de los sistemas de base de datos podemos mencionar:

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por parte de múltiples usuarios.
- Integridad de los datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.
- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.

3.3 Sistema de Gestión de Base de Datos (SGBD)

Los Sistemas de Gestión de Base de Datos (en inglés DataBase Management System) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

3.4 Ventajas de las bases de datos

Control sobre la redundancia de datos: Los sistemas de ficheros almacenan varias copias de los mismos datos en ficheros distintos. Esto hace que se desperdicie espacio de almacenamiento, además de provocar la falta de consistencia de datos.

*Base de Datos II
†Juan Rodriguez Mamani

UNIVERSIDAD PRIVADA DE TACNA, Diciembre 2018, Tacna - Perú

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Consistencia de datos: Eliminando o controlando las redundancias de datos se reduce en gran medida el riesgo de que haya inconsistencias. Si un dato está almacenado una sola vez, cualquier actualización se debe realizar sólo una vez, y está disponible para todos los usuarios inmediatamente. Si un dato está duplicado y el sistema conoce esta redundancia, el propio sistema puede encargarse de garantizar que todas las copias se mantienen consistentes.

Compartir datos: En los sistemas de ficheros, los ficheros pertenecen a las personas o a los departamentos que los utilizan. Pero en los sistemas de bases de datos, la base de datos pertenece a la empresa y puede ser compartida por todos los usuarios que estén autorizados.

Mantenimiento de estándares: Gracias a la integración es más fácil respetar los estándares necesarios, tanto los establecidos a nivel de la empresa como los nacionales e internacionales. Estos estándares pueden establecerse sobre el formato de los datos para facilitar su intercambio, pueden ser estándares de documentación, procedimientos de actualización y también reglas de acceso.

Mejora en la integridad de datos: La integridad de la base de datos se refiere a la validez y la consistencia de los datos almacenados. Normalmente, la integridad se expresa mediante restricciones o reglas que no se pueden violar. Estas restricciones se pueden aplicar tanto a los datos, como a sus relaciones, y es el SGBD quien se debe encargar de mantenerlas.

Mejora en la seguridad: La seguridad de la base de datos es la protección de la base de datos frente a usuarios no autorizados. Sin unas buenas medidas de seguridad, la integración de datos en los sistemas de bases de datos hace que éstos sean más vulnerables que en los sistemas de ficheros.

4 ANÁLISIS

Esta lista de verificación fue desarrollada por los administradores del sistema IST para proporcionar una guía para proteger las bases de datos que almacenan datos confidenciales o restringidos. La implementación de estos controles de seguridad ayudará a evitar la pérdida de datos, la fuga o el acceso no autorizado a sus bases de datos.

4.1 Seguridad de servidor de base de datos física

La máquina física que aloja una base de datos se encuentra en un entorno seguro, bloqueado y supervisado para evitar la entrada no autorizada, el acceso o el robo.
Los servidores de aplicaciones y web no están alojados en la misma máquina que el servidor de base de datos.

4.2 Cortafuegos para servidores de base de datos

• El servidor de la base de datos se encuentra detrás de un firewall con reglas predeterminadas para denegar todo el tráfico.
• El servidor de seguridad del servidor de base de datos se abre solo para aplicaciones específicas o servidores web, y las reglas del servidor de seguridad no permiten el acceso directo del cliente. Si el entorno de desarrollo no puede cumplir con este requisito, los datos restringidos no se almacenan en el servidor de la base de datos de desarrollo y los datos simulados se componen para el desarrollo. La ofuscación de datos de datos de producción no es suficiente.
• Los procedimientos de control de cambio de reglas de firewall están en su lugar y la notificación de los cambios de reglas se distribuye a los administradores de sistemas (SA) y administradores de bases de datos (DBA).
• Las reglas de cortafuegos para servidores de bases de datos se mantienen y revisan de forma regular por los SA y los DBA. Si utiliza el servicio de firewall provisto por IST, las reglas también son revisadas regularmente por Information Security and Polic (ISP).
• Pruebe regularmente el endurecimiento de la máquina y las reglas del firewall a través de las exploraciones de la red, o permitiendo las exploraciones del ISP a través del firewall.

4.3 Software de base de datos

• La versión del software de la base de datos actualmente es compatible con el proveedor o el proyecto de código abierto, según lo exigen los estándares de seguridad mínimos del campus.
• Todos los servicios o funciones no utilizados o innecesarios de la base de datos se eliminan o desactivan.
• Las cuentas predeterminadas innecesarias se eliminan o las contraseñas se cambian de las predeterminadas.
• Las contraseñas nulas no se utilizan y los archivos temporales del proceso de instalación que pueden contener contraseñas se eliminan.
• El software de la base de datos está parcheado para incluir todos los parches de seguridad actuales. Se establecen disposiciones para mantener los niveles de parches de seguridad de manera oportuna.

4.4 Aplicación / Servidores Web / Código de Aplicación

• Los sistemas de destino (aplicación / servidores web) que reciben datos restringidos se protegen de una manera proporcional a las medidas de seguridad en el sistema de origen.
• Todos los servidores y clientes cumplen con los estándares mínimos de seguridad.
• Todos los servidores, aplicaciones y herramientas que acceden a la base de datos están documentados.
• Los archivos de configuración y el código fuente están bloqueados y solo son accesibles para las cuentas de SO requeridas.
• El código de la aplicación se revisa para detectar vulnerabilidades de inyección SQL. No se permite "Spyware" en los servidores de aplicaciones, web o bases de datos.

4.5 Estaciones de trabajo de usuario / cliente

• Si a los usuarios se les permite datos restringidos en sus estaciones de trabajo, las estaciones de trabajo cliente cumplen con los estándares mínimos de seguridad.
• Si a los usuarios se les permite datos restringidos en sus estaciones de trabajo, entonces la estación de trabajo está protegida contra el acceso no autorizado a una sesión mediante la implementación de protectores de pantalla. Los usuarios entienden el requisito de bloquear sus estaciones de trabajo al salir de la estación.
• Si a los usuarios se les permite datos restringidos en sus estaciones

de trabajo, entonces la estación de trabajo debe requerir un inicio de sesión y una contraseña individuales.
• Si a los usuarios se les permite datos restringidos en sus estaciones de trabajo, entonces el sistema operativo de la estación de trabajo encriptará los datos restringidos en la estación de trabajo cliente.
• Los datos restringidos no se almacenan en dispositivos transportables.
• Los datos restringidos nunca se envían por correo electrónico, ya sea en el cuerpo o como un archivo adjunto, ni por los usuarios ni como parte automatizada del sistema.
• Los datos restringidos que ya no son necesarios se eliminan de forma rutinaria.
• Si a los usuarios se les permite datos restringidos en sus estaciones de trabajo, entonces no se permite "Spyware" en las estaciones de trabajo cliente.

4.6 Administrador de cuentas / permisos / contraseñas

• Los DBA entienden su responsabilidad de revisar todos los cambios solicitados en la base de datos y los scripts para garantizar que la seguridad del sistema no se vea comprometida.
• Las cuentas con capacidades de administración del sistema se proporcionan a la menor cantidad de personas que sean prácticas y solo cuando sea necesario para respaldar la aplicación.
• Todos los desarrolladores, proveedores, SA, DBA y contratistas han firmado un acuerdo de confidencialidad.
• Las cuentas del sistema operativo utilizadas por el personal de DBA para iniciar sesión en las máquinas del servidor de datos para tareas administrativas son cuentas individuales y no una cuenta de grupo compartida.
• Cuando sea posible, la cuenta del sistema operativo del daemon que se requiere para ejecutar el proceso del servidor de datos no permite un inicio de sesión directo.
• En su lugar, las cuentas individuales del sistema operativo se utilizan para iniciar sesión, luego sudo o su para la cuenta daemon (para UNIX) o no permitir el inicio de sesión de escritorio (Windows).
• Las cuentas de base de datos utilizadas por el personal de DBA para tareas administrativas son cuentas individuales y no una cuenta de grupo compartida.
• Se permite una cuenta de grupo para ejecutar trabajos automatizados de mantenimiento y supervisión de DBA, como copias de seguridad.
• El grupo de DBA no utiliza esta cuenta de grupo para tareas interactivas diarias, excepto cuando es necesario para solucionar problemas de mantenimiento y supervisión de trabajos.
• Las contraseñas para todas las cuentas del sistema operativo DBA y las cuentas de base de datos son contraseñas seguras y se cambian cuando los administradores / contratistas dejan sus puestos.
• Si el DBA y las funciones de desarrollador están siendo ocupadas por una sola persona, los cambios son aprobados por el Propietario de los datos.

4.7 Funciones de la base de datos de usuarios / Permisos / Contraseñas / Gestión y generación de informes

• Se utiliza la autenticación segura a la base de datos.
• El procedimiento para aprovisionar y revisar el acceso a la base de datos está documentado. El titular de los datos ha firmado el documento de trámites.
• Sólo los usuarios autorizados tienen acceso a la base de datos.
• A los usuarios se les otorgan los permisos mínimos necesarios para su función de trabajo en la base de datos. Los permisos se administran a través de roles o grupos, y no mediante concesiones directas a las ID de usuario cuando sea posible.
• Las contraseñas seguras en la base de datos se aplican cuando es técnicamente posible, y las contraseñas de la base de datos se cifran cuando se almacenan en la base de datos o se transmiten a través de la red.
• Las aplicaciones requieren inicio de sesión de base de datos individual / contraseña y roles / subvenciones cuando sea posible. Cuando no es posible, las cuentas de la aplicación pueden ser utilizadas. Sin embargo, el ID de inicio de sesión y la contraseña deben estar protegidos en este caso, y esta información no existe en la estación de trabajo cliente.
• Las aplicaciones deben administrar los permisos y auditorías de los usuarios para cumplir con los requisitos de los Propietarios de datos.
• Los objetos de la base de datos de usuarios con datos restringidos no tienen subvenciones públicas cuando es posible. Documentar cualquier subvención pública si es necesario en bases de datos con datos restringidos.
• Las cuentas que no pertenecen a DBA no permiten la concesión de roles o permisos en ningún entorno con datos restringidos (control de calidad, producción, desarrollo).
• Las cuentas de la base de datos se bloquean después de un máximo de seis inicios de sesión fallidos.
• El propietario de los datos documenta y aprueba el procedimiento para dirigirse a los usuarios inactivos.
• Los DBAs proporcionan un informe de permisos de base de datos elevados al propietario de los datos trimestralmente.
• Un informe de todos los derechos de acceso para los usuarios es proporcionado al propietario de los datos por los DBA de forma regular. Dos veces al año es el intervalo recomendado.

4.8 Datos restringidos

Solo los datos restringidos requeridos para la función comercial se mantienen dentro de la base de datos. Cuando es posible, la información histórica se elimina cuando ya no es necesaria. La redundancia de datos restringidos se elimina en todo el sistema, y se evita la ocultación de datos restringidos fuera del sistema de registro siempre que sea posible. Las funciones de hash se aplican a elementos de datos restringidos antes de almacenarlos si los datos solo se requieren para propósitos de coincidencia. Si es posible, disocie los datos restringidos de la información de identificación personal y manténgalos fuera de línea hasta que sea necesario. Si se requieren transferencias de datos para otras aplicaciones, notifíqueles los datos restringidos y sus requisitos de seguridad. Los datos restringidos en entornos no productivos se mantienen bajo

los mismos estándares de seguridad que los sistemas de producción. En los casos en que los entornos que no son de producción no se mantienen en el mismo estándar de seguridad que el requerido en la producción, los datos en estos entornos que no son de producción deben cifrarse utilizando algoritmos estándar de la industria, o bien los datos de prueba deben estar compuestos por estos sistemas. La ofuscación de datos no es suficiente. Los elementos de datos restringidos dentro de la base de datos están documentados. Los datos restringidos nunca se utilizan como una clave en una tabla.

4.9 Gestión del cambio

Los procedimientos de gestión de cambios están documentados y cumplen con los requisitos del propietario de los datos. Los controles de administración de cambios están implementados para registrar todos los cambios en la base de datos de producción. Todos los programas programados para ejecutarse en la base de datos que lee o modifica los datos de producción están documentados.

4.10 Auditoria de base de datos

Todos los inicios de sesión en el sistema operativo y los servidores de base de datos, exitosos o no, se registran. Estos registros se conservan durante al menos un año. Los objetos de la base de datos con datos restringidos tienen la auditoría activada cuando sea técnicamente posible. Los registros de auditoría son revisados regularmente por personas informadas e independientes designadas por el propietario de los datos para cumplir con los requisitos del propietario de los datos. Estos requisitos y el proceso de revisión están documentados. Las cuentas que están bloqueadas debido a errores máximos de inicio de sesión en la base de datos activan una notificación automática de los administradores de seguridad responsables de este sistema.

4.11 Copia de seguridad y recuperación de la base de datos

Los procedimientos de copia de seguridad y recuperación están documentados y cumplen con los requisitos del propietario de los datos. Los procedimientos de copia de seguridad y recuperación se prueban periódicamente. Los intervalos de retención de copia de seguridad están documentados y son suficientes para cumplir con los requisitos de reanudación empresarial y las expectativas del propietario de los datos.

4.12 Cifrado de base de datos y gestión de claves

Los datos restringidos se cifran durante la transmisión a través de la red utilizando medidas de encriptación lo suficientemente sólidas para minimizar el riesgo de exposición de los datos si se los intercepta o se envía incorrectamente de la base de datos a la estación de trabajo cliente.
Si se implementa el cifrado a nivel de base de datos para datos restringidos, se documentan los procedimientos para la administración segura de claves. (Consulte las recomendaciones actuales en el Instituto Nacional de Estándares y Tecnología (NIST)). Nota: Se recomienda que todas las capas de aplicación (red, aplicación, estación de trabajo cliente) ya estén cifradas antes de cifrar la base de datos. El cifrado de la base de datos no sustituye ninguno de los requisitos anteriores. El cifrado de la base de datos de datos restringidos no es obligatorio para cumplir con este documento de estándares.
Para los datos sujetos a divulgación que están cifrados en el almacenamiento, los medios para descifrar deben estar disponibles para más de una persona y aprobados por el propietario de los datos.
Las cintas de copia de seguridad almacenan las copias de seguridad de la base de datos en un formato cifrado, y las cintas no almacenan las claves de cifrado de texto sin formato necesarias para descifrar las copias de seguridad.
Los procedimientos de administración de claves para descifrar copias de seguridad están documentados, disponibles para más de una persona y aprobados por el propietario de los datos.

5 CONCLUSIONES

• Los datos de cualquier organización son una propiedad muy valiosa.
• La seguridad de los datos confidenciales es siempre un gran desafío para una organización en cualquier nivel.
• Las bases de datos son un objetivo favorito de los atacantes debido a sus datos. Hay muchas maneras en que una base de datos puede ser comprometida.
• Existen varios tipos de ataques y amenazas a partir de los cuales se debe proteger una base de datos.
• Para asegurar los datos que consideraciones debemos tener en cuenta, se mencionan en este documento y todas las técnicas que se utilizan recientemente para la seguridad de la base de datos.

REFERENCES

[1] La importancia de la seguridad e integridad en base de datos. https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/la-importancia-de-la-seguridad-e-integridad-en-base-de-datos

[2] ¿Qué son las bases de datos? http://www.maestrosdelweb.com/que-son-las-bases-de-datos

[3] Database Hardening Best Practices. https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/database-hardening-best-practices

[4] 7 Database Security Best Practices https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/database-hardening-best-practices

[5] Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009.

[6] 2012 future of cloud computing survey results – North Bridge http://northbridge.com/2012-cloud-computingsurvey.

[7] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,‖Database Security and Encryption: A Survey Study‖, International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.