AMENAZAS A LAS BASES DE DATOS

DICKSON ARLEY GARCIA RINCON

SENA

SERVICIO NACIONAL DE APRENDIZAJE

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

MEDELLIN

2019

**INTRODUCCIÓN**

La seguridad informatica se encarga de velar por la protecion de la informacion en la organización. Tambien por la integirdad de los equipos de informaticos, identificando y eliminando vulnerabilidades. Uno de los activos mas valiosos en las empresas es la información, la perdida de informción tiene un costo mas elevado que el valor de sus equipos.

La mayoria de esta informacion se encuentra en sistemas gestores de bases de datos como Oracle, MySQL, Microsoft SQL Server, MongoDB, Cassandra, SQLite, MariaDB, PostgreSQL, entre otros. A medida que la extructura organizacional crece la cantidad de datos tambien crece en estos sistemas y se debe mantener estos datos con la mayor integridad posible.

En este informe veremos, ¿Por qué son tan vulnerables las bases de datos? Y analizaremos dos de las diez amenazas principales mas comunes, dando una breve definicion y como podriamos protegernos de estos ataques.

**¿Por qué son tan vulnerables las bases de datos?**

La informacion mas sensible de las empresas se encuentra en los sistemas gestores de base de datos, alli se almacen las transacciones comerciales, facturacion, cobranza, informacion, contactos de clientes y usuarios. Si un ataque logra superar las sistemas de seguridad las perdidas seria invaluables, es por esto que las bases de datos son el blanco principal para los hackers. Existes diferentes amenazas a las bases de datos entre las primeras 10 tenemos:

1. Privilegios excesivos y privilegios no utilizados.

2. Abuso de privilegios legítimos.

3. Inyección SQL.

4. Malware.

5. Proceso de auditoría débil.

6. Exposición de los medios de almacenamiento.

7. Explotación de vulnerabilidades y bases de datos mal configuradas.

8. Datos sensibles no administrados.

9. Negación o denegación de servicios.

10. Educación y experiencia limitada en seguridad.

De las 10 amenazas mas frecuentes en bases de datos mencionadas anteriormente, tomaremos 2 de ellas (Inyeccion SQL y Malware) para analizarlas y tomar algunas prevenciones a posibles ataques.

**Inyeccion SQL**

Hoy día todas las aplicaciones web hace uso de base de datos para ofrecer una mejor interacion con el usuario y una navegacion dinamica almacenado datos tanto de informacion con de los usuarios. Un ataque de inyeccion de SQL, implica a un usuario que busca y se aprovecha de la vulnerabilidades que tenga una aplicación para enviar consultas de datos no autorizadas. Saltan los procesos de validacion de privilegios y obtiene datos de otras cuentas de usuario para eliminarlos, modificarlos, copiarlos o tambien secuestrarlos y luego cobrar por regresar el control. El éxito de un ataque de inyeccion SQL es si una usuario logra acceder a la base de datos completa sin ninguna restriccion.

El éxito de un ataque de inyección SQL puede dar a alguien acceso sin restricciones a una base de datos completa. Si las secuencias inyectadas son ejecutadas a través de la base de datos, almacenes de datos críticos pueden ser visualizados, copiados o modificados.

Para prevenir estos ataques, se debe realizar auditorias a las bases de datos, verificar los controles de acceso y deteccion de consultas no autorizadas inyectadas a travez de aplicaciones web. Otro control para mejorar la seguridad en la base de datos es limitar el acceso a la base de datos. Se debe limitar el acceso a los datos sencible, tambien los procedimientos importantes limitarlo a usuarios especificos.

Identificar los datos sensible y datos criticos ayuda a no gastar esfuerzo, tiempo y recursos. Luego de identificados los datos sensibles y la informacion confidencial se puede utilizar algoritmos para cifrado de datos, en caso de que un atacante supere las barreras de proteccion y tenga acceso a los datos estos esten cifrados. Se debe auditar y registrar las acciones y movimientos de los datos. Cuando se tiene un historial completo de las transacciones se puede visualizar mejor los patrones en el acceso y evitar fugas de informacion.

Recuerda seguir estos consejos y ser muy precavido a la hora de administrar y proteger tus bases de datos. La información que estas alojan es muy valiosa para la empresa y un botín codiciado para los atacantes, por lo que sin dudas merece toda tu atención.