Tarea 1

Valeria C. Campos Hdz.

Instituto Tecnológico de Pabellón de Arteaga

Seguridad en Bases de Datos

Efrén Emmanuel Prado López

3 de febrero de 2023

Tarea: Investigar los principales problemas de seguridad en bases de datos.

1. Gestión inadecuada de accesos

Muchas bases de datos residen dentro de su propia máquina y ésta debe estar lo más protegida y bloqueada posible. Solo deben poder acceder como administrador de base de datos los usuarios imprescindibles, y los inicios de sesión deben estar limitados a un estrecho rango de redes y otras máquinas. Los firewalls pueden bloquear direcciones IP. Las mismas reglas deberían aplicarse también a la capa del sistema operativo y, si se ejecuta en una máquina virtual, al hipervisor o la administración de la nube. Estas restricciones ralentizarán el trabajo de actualización de software y la solución de problemas, pero vale la pena restringir los caminos que pueden tomar los atacantes.

2. Fácil acceso físico

No se sabe qué podría hacer un atacante inteligente dentro de la sala de servidores. Las empresas de la nube y las instalaciones de coubicación ofrecen jaulas cerradas dentro de edificios fuertemente vigilados con acceso limitado. Si sus datos son almacenados de manera local en su centro de datos, siga las mismas reglas asegurándose de que solo la gente de confianza tenga acceso a la sala que contiene las unidades de disco físicas.

3. Copias de seguridad desprotegidas

No es raro que un equipo haga un gran trabajo asegurando un servidor de base de datos, pero luego se olvide de las copias de seguridad. Contienen la misma información, así que necesitan el mismo cuidado. Las cintas, unidades y otros medios estáticos deben guardarse en una caja fuerte, preferiblemente en otro lugar donde no se puedan dañar con la misma catástrofe que destruya los originales.

4. Información Minera Clasificada

En general los datos dentro de un sistema están protegidos, sobre todo en las ubicaciones de entrada y salida. Sin este control, las empresas rivales, los profesionales de tecnología corruptos y los hackers, pueden explotar los datos del sistema poco protegidos y venderlos para su beneficio.

Por ejemplo, si los datos vulnerados están relacionadas al lanzamiento de un nuevo producto, esto puede incurrir es pérdidas para el negocio. Estos datos deben protegerse, agregando varias capas de seguridad, incluida la anonimización.

Si los datos que consiguen los ciberdelincuentes no tienen información personas como nombres o números telefónicos, no podrá hacer daño.

5. Ingeniería Social

Este es uno de los problemas más difíciles de identificar, ya que son métodos no técnicos que tiene un hacker para conseguir acceso a tu sistema o datos, ya sea para robarlos o dañarlos.

Aquí es donde vemos los correos electrónicos sospechosos, donde el método es la mentira para ganar confianza y conseguir el objetivo. El phishing es un mensaje o un correo electrónico que te envían para sacarte información y robar tus datos, por lo general bancarios.
Estos ataques son efectivos porque son personas y no un programa los que están detrás de estos. A través de la persuasión y el engaño, logran conseguir lo que quieren. Estas personas, por ejemplo, se hacen pasar por un amigo, por un agente bancario y su actuación es lo que les permite lograr su objetivo.

References

(s.f.). Obtenido de https://cioperu.pe/articulo/33054/12-fallas-y-errores-de-seguridad-de-las-bases-de-datos/

(s.f.). Obtenido de https://revistaempresarial.com/tecnologia/seguridad-informatica/los-5-principales-problemas-de-seguridad-de-datos-que-debes-solucionar-de-inmediato/