**Amenazas, riesgos y vulnerabilidades de bases de datos SQL.**

**Gestión de permisos inadecuada**

Más a menudo de lo que nos gustaría admitir, los servidores de bases de datos se instalan en organizaciones con su configuración de seguridad predeterminada y esta configuración nunca se cambia. Esto hace que las bases de datos queden expuestas a atacantes que conocen los permisos predeterminados y saben cómo explotarlos.

**Ataques de inyección de base de datos**

La principal forma de ataques de inyección de base de datos es inyección SQL ataques, que atacan servidores de bases de datos relacionales (RDBMS) que utilizan lenguaje SQL. Las bases de datos NoSQL, como MongoDB, RavenDB o Couchbase, son inmunes a los ataques de inyección SQL pero son susceptibles a los ataques de inyección NoSQL. Los ataques de inyección NoSQL son menos comunes, pero igualmente peligrosos.

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.

**Vulnerabilidades de bases de datos explotables**

Es común que los departamentos de TI corporativos no apliquen parches a su software principal de DBMS con regularidad. Por lo tanto, incluso si se descubre una vulnerabilidad y el proveedor lanza un parche para eliminarla, pueden pasar meses antes de que las empresas parcheen sus sistemas. El resultado es que las vulnerabilidades quedan expuestas durante largos períodos, lo que puede ser aprovechado por los ciberdelincuentes.

**Existencia de servidores de bases de datos ocultos**

El incumplimiento de las políticas de instalación de software en una organización (o la falta de tales políticas) hace que los usuarios instalen servidores de bases de datos a su discreción para resolver necesidades particulares. El resultado es que aparecen servidores en la red de la organización, algo que los administradores de seguridad desconocen. Estos servidores exponen datos confidenciales a la organización o exponen vulnerabilidades que los atacantes pueden aprovechar.

**Copias de seguridad accesibles**

Aunque los servidores de bases de datos están protegidos por una capa de seguridad, los usuarios sin privilegios pueden acceder a las copias de seguridad de estas bases de datos. En tal situación, existe el riesgo de que usuarios no autorizados puedan hacer copias de las copias de seguridad y montarlas en sus propios servidores para extraer la información confidencial que contienen.

**Falta de contingencia**

Las empresas que se jactan de ser “ágiles” y “receptivas”, a menudo alcanzan esa velocidad mediante el abandono de la estandarización, los procesos maduros y el planeamiento de contingencias. Muchas PyMEs descubrieron que un simple fallo o compromiso de los datos se convierte en un desastre cuando no hay Plan de Continuidad de Negocios, Plan de Recuperación ante Desastres, Política de Respuesta ante Intrusiones, sistema de respaldo actualizado desde el cual realmente se pueda hacer una recuperación o almacenamiento en otra ubicación.

**Correo electrónico HTML malicioso**

El ataque más común por correo electrónico ahora viene como un mensaje en HTML que contiene un enlace hacia un sitio malicioso con alguna trampa caza bobos. Un clic equivocado puede desencadenar una descarga peligrosa. Los riesgos son los mismos que en la Amenaza # 3, "Navegación web imprudente”, pero el atacante utiliza el correo electrónico para llevar a la víctima hacia su sitio web malicioso.

**Uso temerario de redes de hoteles y quioscos**

Las redes de los hoteles están notoriamente infectadas con virus, gusanos, spyware y malware y, a menudo, funcionan con malas prácticas globales de seguridad. Los quioscos públicos son un lugar conveniente para que un atacante deje un keylogger, sólo para ver qué cae en su red. Las laptops que no tengan software de firewall personal, antivirus y antispyware pueden verse comprometidas cuando están de viaje. Las defensas tradicionales pueden volverse inútiles cuando el usuario, literalmente, transporta la laptop a lo largo del gateway firewall y se conecta desde el interior de la zona confiable.

**Solución los problemas.**

Para brindar una protección adecuada a las bases de datos de una organización, se necesita una matriz defensiva de mejores prácticas, combinada con controles internos regulares. La matriz de mejores prácticas incluye los siguientes elementos:

* Administre los derechos de acceso de los usuarios y elimine los privilegios excesivos y los usuarios inactivos.
* Capacite a los empleados en técnicas de mitigación de riesgos, incluido el reconocimiento de amenazas cibernéticas comunes, como ataques de phishing, las mejores prácticas en torno al uso de Internet y correo electrónico, y [gestión de contraseñas](https://geekflare.com/es/secure-password-with-1password/).
* Evalúe las vulnerabilidades de la base de datos, identifique los puntos finales comprometidos y clasifique los datos confidenciales.
* Supervise toda la actividad de acceso a la base de datos y los patrones de uso en tiempo real para detectar fugas de datos, SQL no autorizado y [Big Data](https://geekflare.com/es/big-data-tools-for-data-scientist/) transacciones y ataques de protocolo/sistema.
* Automatice la auditoría con una plataforma de auditoría y protección de bases de datos.
* Bloquee las solicitudes web maliciosas.
* Archivar datos externos, [cifrar bases de datos](https://geekflare.com/es/data-encryption-terminology/)y enmascare los campos de la base de datos para ocultar información confidencial.

**También es posible utilizar herramientas para facilitar este trabajo.**

* Scuba Database Vulnerability Scanner
* dbWatch Control Center.
* AppDetectivePRO.
* DbDefence.
* OScanner.
* dbForge Security Manager.