Gonzalo Vaca

Gonzalo Rodríguez

Pablo Martín

Jaime Sánchez

Pablo Pradillo

Edu Carro

Javi Santabárbara

Hugo Lobo

**ANÁLISIS DE RIESGOS A LA HORA DE IMPLEMENTAR LA SOLUCIÓN**

Inicialmente, un análisis de riesgos se define como aquel proceso destinado a mitigar el impacto de los riesgos en las operaciones empresariales. Principalmente, los diferentes sectores utilizan dicho proceso para gestionar correctamente los posibles problemas que puedan surgir en la empresa, con el fin de obtener un panorama realista que considere tanto lo positivo como lo negativo.

En el caso de la base de datos; implementar un análisis de riesgos puede llegar a ser una labor muy compleja, debido a que, los requisitos de seguridad cambian constantemente, lo cual dificulta a la creación de un sólido análisis de riesgos. No obstante, en relación con dicho caso, podemos identificar una serie de riesgos que amenazan de forma directa a la propia base de datos:

- Contraseñas vulnerables.

- No implementación de parches actualizados.

- Archivos vulnerables de los sistemas operativos subyacentes.

- Corrupta utilización de privilegios concedidos para el acceso a la base de datos.

- No auditoría del acceso a la base de datos.

En cuanto a las contraseñas vulnerables, se identifican como aquellas contraseñas débiles, predeterminadas o fáciles de adivinar y como uno de los mayores riesgos de seguridad debido a su facilidad de predicción. Dichas contraseñas predeterminadas se envían, a través de, un sistema de base de datos cuyos ajustes predeterminados son bastante conocidos, lo cual implica que si no se modifican, son suficientemente accesibles. Por lo tanto, para poder garantizar contraseñas lo suficientemente seguras para el usuario (y en consecuencia, anular dicho riesgo mencionado anteriormente); es necesario aplicar las siguientes posibles soluciones:

- La contraseña elegida debe ser distinta a la predeterminada y al nombre del usuario.

- La contraseña elegida debe contener una mezcla de letras, caracteres y números.

- La contraseña elegida debe tener una longitud suficiente.

- Se debe de realizar cambios de contraseña de forma regular.

- La contraseña elegida no debe de adivinarse fácilmente (fecha de cumpleaños, nombre del usuario... son ejemplos de contraseñas sencillas)

En relación con la no implementación de parches actualizados, se basa en no ejecutar paquetes de servicio (colección de actualizaciones, mejoras de software...), soluciones calientes (corrigen agujeros de seguridad recién descubiertos), correcciones de datos... los cuales contienen correcciones de errores y actualizaciones de seguridad esenciales para mantener sistemas de bases de datos seguros. Por lo tanto, para poder implementar parches actualizados que aumenten la seguridad de nuestra base de datos (y en consecuencia, anular dicho riesgo mencionado anteriormente); es necesario aplicar las siguientes posibles soluciones:

- Ejecución de paquetes de servicio.

- Ejecución de soluciones calientes.

- Ejecución de correcciones de datos.

Con respecto a los archivos vulnerables de los sistemas operativos subyacentes; se identifican como aquellos archivos que presentan un gran potencial de provocar un acceso no autorizado a los datos y a la corrupción de ellos mismos (acceso a la lectura de archivos de la base de datos, bloqueo de contraseñas y controles de acceso...). Por lo tanto, para poder garantizar unos sistemas operativos subyacentes eficientes (y en consecuencia, anular dicho riesgo mencionado anteriormente); es necesario aplicar la siguiente posible solución:

- Los permisos y la configuración de los archivos de los sistemas operativos subyacentes deben ser coherente con las políticas generales de seguridad de la base de datos de la organización.

En consideración a la corrupta utilización de privilegios concedidos para el acceso a la base de datos, se basa en el proceso mediante el cual un cierto número de personas se les conceden privilegios que exceden de sus funciones laborables requeridas, los cuales permiten en acceso abiertos a posibles ataques o a información confidencial. Por lo tanto, para poder garantizar un correcto y seguro acceso a la base de datos (y en consecuencia, anular dicho riesgo mencionado anteriormente); es necesario aplicar la siguiente posible solución:

- Implementación optimizada de programas cuyo objetivo es mejorar y limitar los controles de acceso, identificar usuarios que abusan del acceso legítimo con fines no autorizados...

Finalmente, acerca de la no auditoría del acceso a la base de datos; se basa en no revisar la base de datos, por lo que, dicho proceso genera la incapacidad de analizar los cambios o movimientos de actividad no autorizada. Por lo tanto, para procurar una auditoría correcta y eficiente del acceso a la base de datos (y en consecuencia, anular dicho riesgo mencionado anteriormente), es necesario aplicar la siguiente posible solución:

- Establecer un sistema de gestión el cual audite la base de datos (proporcionan algún nivel de capacidad de revisión de bases de datos nativas). Sin embargo, este tipo de sistema gestor, frecuentemente se desactiva (lo cual no es la mejor opción) por lo que las organizaciones pueden añadir una solución de terceros para aumentar dichas capacidades de auditoría.

- **FUENTES UTILIZADAS**

- https://www.dbta.com/Editorial/Trends-and-Applications/Simple-Steps-to-Reduce-Risk-Database-Risk-51550.aspx

- https://www.oracle.com/security/database-security/