arsys

Cómo garantizar la seguridad de las bases de datos empresariales

La seguridad de las bases de datos empresariales es una prioridad para cualquier organización. Aquí os damos una guía de buenas prácticas.

Mantener los datos seguros es una de las principales preocupaciones de cualquier organización. Cada vez son más las empresas basadas en datos, es decir, aquellas que se centran en tomar sus decisiones a partir de los datos, en vez de hacerlo a partir de la experiencia, la intuición o en modelos preestablecidos. Además, estas empresas están decididas a automatizar sus decisiones eliminando o reduciendo al mínimo la intervención humana.

El enfoque de una empresa basada en datos es completo: no se trata de utilizar algunas herramientas y hacer algunos cálculos o análisis esporádicos. Se desarrolla una cultura que tiene a la información en el centro de todo, y todos los individuos en la organización trabajan para explotarla y extraer valor.

Como ya comentamos, mantener los datos seguros es importante para cualquier empresa, pero en el caso de las empresas basadas en datos, la cuestión es vital. La ciberseguridad es tan importante como disponer de un buen sistema de base de datos, software de análisis de vanguardia o un almacenamiento rápido y eficiente. Muchas bases de datos empresariales están expuestas a vulnerabilidades causadas por errores de configuración, implementaciones deficientes y contraseñas débiles. Sin olvidar los ataques de inyección SQL y las vulnerabilidades de secuencias de comandos entre sitios. Sin embargo, los mayores esfuerzos de protección deben ir dirigidos a proteger los datos más valiosos: los datos confidenciales de los clientes.

¿Cómo mantener segura nuestra base de datos empresarial?

Hacer cumplir el principio del menor privilegio es una de las tareas primordiales para mejorar la seguridad de las bases de datos empresariales.

El concepto es sencillo: se trata de limitar el acceso de los usuarios otorgándoles el conjunto más pequeño de privilegios necesarios para llevar a cabo sus funciones. Implementarlo no es tan sencillo, en todo caso. Para hacerlo bien, es necesario plantear una serie de preguntas orientadas a definir correctamente qué conjunto de privilegios necesita cada trabajador. Por ejemplo:

- ¿Los desarrolladores tienen acceso completo a las bases de datos de producción? ¿Es necesario? ¿Basta con que tengan acceso parcial, o no es necesario en absoluto?
- ¿Los ingenieros de sistemas tienen acceso a las bases de datos en los sistemas bajo su cuidado? ¿En qué medida?
- ¿Los administradores de bases de datos tienen acceso completo a todas las bases de datos o solo a aquellas que se encuentran dentro de sus áreas de responsabilidad?

Este principio funciona razonablemente bien porque si limitamos el acceso al máximo posible sin entorpecer las labores de cada profesional, estaremos limitando en la misma medida los riesgos de fallo y, también de ataque, por parte de personas o grupos malintencionados.

Realizar revisiones periódicas de los privilegios de cada miembro del personal, ya que es muy común, en cualquier empresa tecnológica, la acumulación gradual de derechos de acceso más allá de lo que un individuo necesita para hacer su trabajo (lo que se conoce en inglés como *«privilege creep»*).

A medida que el personal, ya sea técnico o no, se mueve entre diferentes puestos o tareas, proyectos o incluso departamentos, los permisos se van acumulando y varían dependiendo de sus responsabilidades.

Al contrario que los nuevos permisos, que se suelen otorgar con rapidez para no perder tiempo en el que se podría estar trabajando, los antiguos permisos no se revisan como deberían. Es decir, no se revocan esos permisos o, al menos, no tan a menudo y eficientemente como se debería.

Esto supone un enorme riesgo para las empresas porque, a pesar de que esos permisos no influyen en el día a día porque están obsoletos, sí pueden ser un problema si la persona que los posee es víctima de un ciberataque de algún tipo. En ese caso, la organización entera sería vulnerable, dependiendo de qué permisos estuvieran asignados a esa persona.

Por tanto, las revisiones periódicas son esenciales, en especial en el caso de los usuarios que tienen acceso directo a la base de datos.

Monitorizar la actividad de la base de datos es vital para entender qué está sucediendo, quién accede a ella y en qué momentos. Es necesario asegurarse de que se ha habilitado la supervisión de la base de datos en todos los sistemas, y que los registros se envían a un repositorio seguro. También conviene establecer reglas de monitorización que vigilen la actividad inusual del usuario, particularmente entre los usuarios con acceso administrativo.

Cifrar datos confidenciales es una práctica totalmente recomendada en seguridad de bases de datos. Es necesario utilizar un cifrado seguro para proteger las bases de datos de tres maneras:

- Que todas las conexiones de la base de datos utilicen el cifrado de seguridad de la capa de transporte para proteger los datos en tránsito.
- Cifrar los discos que contienen almacenes de datos para protegerlos contra su pérdida, robo o eliminación inadecuada.
- Emplear capacidades de cifrado a nivel de columna para proteger los campos de la base de datos más sensibles.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/