arsys

Las mejores prácticas para la revisión del control de acceso de los usuarios

La gestión y el control de acceso de los usuarios es una de las principales herramientas de seguridad en las empresas.

La gestión del acceso de los usuarios a las redes empresariales es un tema importante en seguridad. Hablamos no sólo de controlar qué usuarios acceden a qué recursos (y cuándo), sino también de gestionar las contraseñas, renovarlas, revocarlas cuando ya no son necesarias, y muchas otras acciones.

Existen muchos mecanismos de gestión de identidades y controles de acceso, entre ellos el basado en roles o el principio de mínimo privilegio. Cualquier mecanismo probado es garantía de que podemos controlar los accesos con seguridad, pero, ¿cuántos empleados han dejado la empresa? ¿Cuántos han cambiado de departamento o asumido más responsabilidades? Cuanto más grande es la empresa, más movimientos de este tipo se van a dar a lo largo del año.

Esto impacta directamente en los datos, aplicaciones y sistemas a los que esos empleados tenían o tienen acceso. En el peor de los casos, los empleados que fueron despedidos pueden seguir accediendo a las informaciones más valiosas de la empresa. Otro riesgo a tener en cuenta es la acumulación de privilegios de usuario.

Los riesgos más comunes relacionados con el control de acceso de los usuarios son:

- La acumulación de privilegios.
- Los accesos inapropiados o no autorizados.
- Los intentos de fraude.
- El abuso de privilegios de acceso.
- Las amenazas internas, maliciosas y accidentales.
- La mala configuración de las cuentas.
- Las políticas de acceso de usuarios obsoletas.

Cómo llevar a cabo una revisión del acceso de los usuarios

Veamos cómo podemos revisar de manera eficiente los controles de acceso de los usuarios para evitar los riesgos asociados a la acumulación de privilegios o la asignación incorrecta de estos.

1 Definir la política de gestión de accesos

Una política de gestión de accesos de usuarios debería incluir:

- **Un inventario de los activos de la empresa**. Deben incluirse todos los activos a los que los diferentes empleados pueden tener privilegios de acceso: Bases de datos, aplicaciones, sistemas, redes, sistemas operativos, centros de datos, salas, edificios, etc.

  Lista de propietarios para cada activo, por ejemplo, un gerente, un administrador o un equipo de TI. Los propietarios deben detallar los tipos de datos y contenidos accesibles en sus activos, que se asignarán a los diferentes niveles de acceso.

- **Descripciones de los niveles de acceso y los roles de los usuarios.** Proporcionar el mínimo privilegio necesario para una función de trabajo es fundamental para eliminar las brechas de seguridad de la identificación del usuario.

- **Frecuencia y tipos de informes.** Las revisiones de acceso de los usuarios pueden realizarse por sistema, por empleado o como una combinación de ambos. Una revisión por sistema auditará los controles de acceso basándose en quién tiene acceso a cada sistema, mientras que una revisión por empleado examina los privilegios basándose en los sistemas a los que accede un empleado.

- **Procesos de desaprovisionamiento.** La política de revisión del acceso de los usuarios debe detallar los procesos corporativos de aprovisionamiento y desaprovisionamiento. El aprovisionamiento explica cómo se asignan los privilegios de acceso a un nuevo empleado. El desaprovisionamiento explica cómo se revocan esos accesos de usuario cuando un empleado cambia de función o es despedido.

2 Llevar a cabo la revisión

Una vez establecida la política es el momento de crear un informe de todas las bases de datos, aplicaciones y sistemas, y aclarar quién tiene actualmente acceso a ellos. Deben incluirse todos los empleados y terceros como vendedores, proveedores de servicios y consultores.

Cada propietario de los activos debe tener una copia del informe para auditar la lista y verificar quién tiene acceso y a qué nivel. Y determinar luego qué privilegios deben ser modificados o revocados.

3 Remediación e informe

Una vez hechas todas las revisiones de acceso se han de ejecutar los cambios. Hay que eliminar cualquier acceso revocado y actualizar los privilegios de los empleados según sea necesario.

Hecho esto, es el mejor momento para evaluar las brechas de seguridad. El informe final también puede medir lo bien que funcionan las políticas de seguridad, así como si las políticas de acceso durante la contratación, la transferencia o la terminación son eficientes y siguen en línea con el modelo de seguridad de su empresa.

En Arsys nos tomamos muy en serio el compliance, y por ello ofrecemos a nuestros clientes servicios de consultoría y asesoramiento IT, así como servicios de seguridad gestionada y unas infraestructuras con los mejores niveles de cumplimiento.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

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

www.instagram.com/arsys.es/