Filtración de datos

INCIDENTE

Un gerente de ventas compartió el acceso a una carpeta de documentos internos con su equipo durante una reunión. La carpeta contenía archivos asociados con un nuevo producto que no se ha anunciado públicamente. También incluyó análisis de clientes y materiales promocionales. Después de la reunión, el gerente no revocó el acceso a la carpeta interna, pero advirtió al equipo que esperará la aprobación antes de compartir los materiales promocionales con otros.

Durante una videollamada con un socio comercial, un miembro del equipo de ventas olvidó la advertencia de su gerente. El representante de ventas tenía la intención de compartir un enlace a los materiales promocionales para que el socio comercial pudiera distribuirlos entre sus clientes. Sin embargo, el representante de ventas compartió accidentalmente un enlace a la carpeta interna. Más tarde, el socio comercial publicó el enlace en la página de redes sociales de su empresa. suponiendo que fueron los materiales promocionales.

TIPO DE CONTROL

Control	Mínimo privilegio
Asuntos)	*El acceso a la carpeta interna no se limitó al equipo de ventas y al gerente. No se debería haber dado permiso al socio comercial para compartir la información promocional en las redes sociales.*
Revisar	*NIST SP 800-53: AC-6 aborda cómo una organización puede proteger la privacidad de sus datos mediante la implementación de privilegios mínimos. También sugiere mejoras de control para mejorar la efectividad del privilegio mínimo.*
Recomendaciones	• *Restrinja el acceso a recursos confidenciales según la función del usuario.* • *Audite periódicamente los privilegios de los usuarios.*

Justificación	*Las fugas de datos se pueden evitar si los enlaces compartidos a archivos internos están restringidos únicamente a los empleados. Además, requiriendo que los gerentes y equipos de seguridad auditen periódicamente el acceso a los archivos del equipo. ayudaría a limitar la exposición de información sensible.*

PLAN DE SEGURIDAD

El NIST Ciberseguridad FRamework (CSF) utiliza una estructura jerárquica en forma de árbol para organizar la información. De izquierda a derecha, describe una función de seguridad amplia y luego se vuelve más específica a medida que se divide en una categoría, subcategoría y controles de seguridad individuales.

Función	Categoría	Subcategoría	Referencia(s)
Proteger	PRDS: *Seguridad de datos*	PR.DS-5: *Protecciones contra fugas de datos.*	NIST SP 800-53: AC-6

En este ejemplo, los controles implementados que utiliza el fabricante para proteger contra fugas de datos se definen en NIST SP 800-53, un conjunto de pautas para proteger la privacidad de los sistemas de información.

NIST SP 800-53: AC-6

NIST desarrolló SP 800-53 para proporcionar a las empresas un plan personalizado para mantener la privacidad de la información. Es un recurso integral que describe una amplia gama de categorías de control. Cada control proporciona algunos datos clave:

- Control: Una definición del control de seguridad.
- Discusión: Una descripción de cómo se debe implementar el control.
- Mejoras de control: Una lista de sugerencias para mejorar la eficacia del control.

AC-6	Mínimo privilegio
	Control: Solo se debe proporcionar a los usuarios el acceso y la autorización mínimos necesarios para completar una tarea o función.
	Discusión: Los procesos, cuentas de usuario y roles deben aplicarse según sea necesario para lograr el mínimo privilegio. La intención es evitar que un usuario opere con niveles de privilegios superiores a los necesarios para lograr los objetivos comerciales.
	Mejoras de control: ● Restrinja el acceso a recursos confidenciales según la función del usuario. ● Revocar automáticamente el acceso a la información después de un período de tiempo. ● Mantenga registros de actividad de las cuentas de usuario aprovisionadas. ● Audite periódicamente los privilegios de los usuarios.