Resumen del incidente

Un gerente de ventas compartió acceso a una carpeta con documentos de uso interno con su equipo durante una reunión. La carpeta contenía archivos relacionados con un nuevo producto que aún no había sido anunciado públicamente. También incluía 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 esperara la aprobación antes de compartir los materiales promocionales con otras personas.

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 pudiera distribuirlos a sus clientes. Sin embargo, el representante 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, asumiendo que se trataba de los materiales promocionales.

Control: Mínimo privilegio (Least privilege)

Problema(s): ¿Qué factores contribuyeron a la filtración de información?

- Acceso excesivo otorgado al equipo sin restricciones basadas en roles.
- Falta de revocación automática del acceso después de la reunión.
- Ausencia de controles que limiten la compartición de enlaces internos.
- Dependencia en advertencias verbales en lugar de controles técnicos.
- Falta de capacitación o recordatorios sobre manejo seguro de información.

Revisión: ¿Qué aborda NIST SP 800-53: AC-6?

AC-6 establece que los usuarios deben recibir **solo el acceso mínimo necesario** para realizar sus tareas. Busca evitar que un usuario opere con privilegios más altos de los requeridos. Incluye prácticas como restringir acceso según roles, revocar accesos automáticamente, registrar actividades y auditar privilegios regularmente.

Recomendación(es): ¿Cómo podría mejorarse el principio de mínimo privilegio en la empresa?

- Implementar controles de acceso basados en roles (RBAC).
- Configurar expiración automática del acceso a carpetas internas.
- Restringir la capacidad de compartir enlaces externos de carpetas internas.
- Registrar y auditar regularmente los permisos otorgados.
- Capacitar al personal sobre manejo seguro de documentos internos.

Justificación: ¿Cómo abordarían estos cambios los problemas identificados?

- Limitar el acceso según roles reduce la probabilidad de que empleados compartan información no destinada a ellos.
- La revocación automática evita que accesos temporales permanezcan activos después de reuniones.
- Las restricciones de compartición previenen errores humanos al enviar enlaces.
- Las auditorías permiten detectar permisos innecesarios o riesgosos.
- La capacitación refuerza la conciencia sobre la importancia de proteger información interna.