Informe de Incidente de Ciberseguridad. Filtración de Datos

1. Resumen del Incidente

- **Tipo de Incidente:**
  Filtración de datos al compartir de manera inapropiada los recursos internos.
- **Descripción del Incidente:**
  Durante una reunión interna, un gerente de ventas compartió el acceso a una carpeta que contenía documentos internos sobre un nuevo producto aún no anunciado públicamente. Aunque advirtió al equipo que no compartiera los materiales hasta obtener la aprobación, no revocó el acceso a la carpeta tras la reunión. Posteriormente, un miembro del equipo de ventas compartió por error un enlace a la carpeta interna con un socio comercial durante una videollamada. El socio, asumiendo que se trataba de material promocional, publicó el enlace en la página de redes sociales de su empresa, exponiendo así información confidencial.

2. Análisis del Incidente

- **Error en la Gestión de Accesos:**
  El acceso a la carpeta interna no fue limitado adecuadamente. Tras la reunión, los permisos de acceso no fueron revocados, lo que permitió que la información permaneciera disponible para el equipo de ventas. El miembro del equipo de ventas, debido a la falta de controles adicionales, compartió el enlace erróneo con el socio comercial.
- **Exposición en Redes Sociales:**
  El socio comercial publicó el enlace a la carpeta interna en sus redes sociales, asumiendo incorrectamente que contenía materiales promocionales aprobados para distribución. Esta acción resultó en una filtración pública de información sensible, incluidos análisis de clientes y detalles sobre el nuevo producto.

3. Tipo de Control Afectado: Principio de Mínimo Privilegio

El control de acceso basado en el principio de mínimo privilegio no se aplicó correctamente. El equipo de ventas recibió acceso sin restricciones temporales o basadas en funciones, lo que permitió que la información fuera compartida de manera accidental con un tercero.

Problemas Identificados:

- Falta de Restricciones:
  El acceso a la carpeta no se restringió adecuadamente tras la reunión.
- Permisos Inapropiados para Terceros:
  No se estableció una política clara que prohibiera compartir la información promocional sin previa aprobación.

4. Recomendaciones de Mejora

1. Restricción Basada en Roles:
   Implementar controles que limiten el acceso a información sensible solo a aquellos usuarios que necesiten dichos datos para sus funciones específicas.
2. Auditoría Periódica:
   Realizar auditorías regulares de los privilegios de acceso de los usuarios para identificar y corregir cualquier exceso de permisos.
3. Revocación Automática de Accesos:
   Configurar sistemas para que revoquen automáticamente el acceso a carpetas sensibles después de un período de tiempo específico o una vez finalizada la tarea para la que fueron concedidos.
4. Capacitación y Concienciación:
   Asegurar que todos los empleados comprendan las políticas de seguridad, especialmente en cuanto a la compartición de documentos y el uso de plataformas de terceros.

5. Plan de Seguridad: Implementación del Marco NIST

El Marco de Ciberseguridad del NIST (CSF) se utiliza para organizar la información y proteger los datos dentro de una empresa. Dentro de este marco, el control AC-6 de Mínimo Privilegio está diseñado para asegurar que los usuarios tengan únicamente los permisos necesarios para realizar su trabajo.

Controles Recomendados:

- Control AC-6: Mínimo Privilegio
  Define que los usuarios deben tener acceso solo a los recursos que necesitan para realizar su trabajo, minimizando la exposición de datos sensibles.
- Mejoras de Control:
  - Limitar el acceso a los recursos confidenciales basados en las funciones de cada usuario.
  - Revocar el acceso a la información tras un período de tiempo.
  - Mantener registros detallados de la actividad de las cuentas de usuario y realizar auditorías periódicas de estos registros.

6. Conclusión

Este incidente pone de manifiesto la necesidad de aplicar controles de seguridad más estrictos, como el principio de mínimo privilegio y la auditoría continua de los accesos a la información. Implementar las recomendaciones proporcionadas, junto con un plan de seguridad basado en el marco NIST, ayudará a prevenir futuras filtraciones de datos y a proteger la información sensible de la organización.