Informe de Políticas de Seguridad: DLP a dispositivos de almacenamiento externo.

1. Introducción

Los dispositivos de almacenamiento externo, como memorias USBs y discos duros externos, se pueden utilizar en TechCorp Solutions para transferir y almacenar datos. Sin embargo, estos dispositivos presentan riesgos significativos de pérdida o filtración de datos si no se gestionan de manera adecuada.

Este informe propone una política de seguridad que limita y controla el uso de este tipo de dispositivos de almacenamiento, aplicando el principio del menor privilegio para garantizar que solo el personal autorizado pueda utilizarlos y acceder a datos sensibles.

2. Clasificación de Datos

Para gestionar adecuadamente los permisos y el uso de dispositivos de almacenamiento externo, TechCorp Solutions clasifica sus datos en tres categorías:

1. **Datos Públicos:** Información general de la empresa que no compromete la seguridad si se transfiere.
2. **Datos Internos:** Información confidencial accesible solo para personal autorizado.
3. **Datos Sensibles:** Datos altamente confidenciales (contratos, acuerdos legales, información financiera, datos de identificación personal...), cuya transferencia solo puede ser realizada por usuarios específicamente autorizados.

3. Acceso y Control (Aplicando Principio del Menor Privilegio)

En línea con el principio del menor privilegio, el uso de dispositivos de almacenamiento externo se gestionará de la siguiente manera:

- **Acceso Restringido:** Solo el personal autorizado podrá conectar y utilizar dispositivos USB en equipos corporativos. El resto de usuarios no podrá conectar este tipo de dispositivos a dichos equipos.
- **Revisión de Permisos:** Los permisos de uso se revisarán trimestralmente para garantizar que solo usuarios activos y autorizados puedan emplear

dispositivos externos. Y siempre tras eventos como despidos, traslados o contrataciones de personal.

- **Acceso Temporal:** Cuando sea necesario transferir datos sensibles, se otorgará acceso temporal mediante autorización formal y se revocará al finalizar la tarea.
- **Restricción de Escritura:** Los dispositivos externos solo podrán configurarse para lectura en la mayoría de los casos, permitiendo escritura únicamente en circunstancias justificadas.

4. **Monitoreo y Auditoría**

Se implementarán políticas de monitoreo y auditoría para detectar el uso indebido de dispositivos de almacenamiento externo:

- **Registro de Actividades:** Se utilizarán herramientas o soluciones DLP para registrar la conexión y el uso de dispositivos USB, incluyendo qué usuarios los conectan y qué archivos se transfieren.
- **Alertas de Seguridad:** Configuración de alertas automáticas para notificar al departamento de IT sobre transferencias de datos sensibles o conexiones no autorizadas.
- **Auditorías Regulares:** Auditorías trimestrales para revisar registros de actividad y detectar posibles incumplimientos de las políticas.

5. **Prevención de Filtraciones**

Para prevenir la filtración de datos a través de dispositivos externos, se aplicarán las siguientes medidas:

- **Bloqueo por Defecto:** Los dispositivos de almacenamiento externo estarán bloqueados de manera predeterminada y requerirán aprobación explícita para su uso.
- **Cifrado Obligatorio:** Todos los datos transferidos a dispositivos externos deberán ser cifrados utilizando AES-256.
- **Control de permisos:** Configuración de permisos para que solo se puedan transferir datos desde carpetas designadas como seguras o solo usuarios autorizados para dicha tarea.

- **Etiquetas de Protección:** Los archivos sensibles estarán etiquetados como "Confidenciales" o "Solo Uso Interno", y su transferencia requerirá permisos adicionales.

6. Educación y Concientización

Es fundamental que los empleados comprendan la importancia de las políticas de seguridad relacionadas con dispositivos externos:

- **Capacitación Obligatoria:** Sesiones semestrales para educar a los empleados sobre el uso seguro de dispositivos externos y las políticas vigentes. También será necesaria una guía con el protocolo de uso entregada a cada nueva contratación.
- **Concientización sobre Riesgos:** Durante las sesiones de capacitación, se presentarán ejemplos de incidentes comunes relacionados con el uso de dispositivos USB (como la pérdida de datos confidenciales, uso indebido de información confidencial, espionaje industrial...) y las mejores prácticas para evitarlos.

7. Conclusión

La implementación adecuada del principio del menor privilegio y las políticas de seguridad propuestas garantizará que TechCorp Solutions minimice los riesgos asociados con dispositivos de almacenamiento externo, protegiendo su información más sensible frente a accesos no autorizados o posibles pérdidas de datos.