Informe de Implementación de Políticas de Seguridad DLP

Índice

Parte 1: Documentación de Políticas DLP

1.1. Principios Fundamentales del DLP

Concepto	Descripción	Aplicación
DLP (Data Loss Prevention)	Conjunto de herramientas y procedimientos diseñados para prevenir la filtración de datos sensibles de la red corporativa. Actúa mediante la identificación de patrones de datos (ej. números de tarjeta de crédito) y el control de los canales de salida (ej. USB, email, nube).	La política implementada se centra en el canal de salida USB.
Clasificación de Datos	Proceso de etiquetar la información según su sensibilidad (Pública, Interna, Sensible/Confidencial). Esta clasificación es el motor que determina qué	Se aplica la restricción total del USB para proteger los **Datos Sensibles** por defecto.

	se debe proteger.	
Principio del Menor Privilegio (PoLP)	Se refiere a que a un usuario, proceso o programa se le deben otorgar sólo los permisos esenciales para realizar su trabajo, y nada más. Esto minimiza la superficie de ataque en caso de compromiso o negligencia.	La implementación debe permitir una regla por defecto de **Denegar** y una excepción muy específica de **Permitir** a un grupo reducido.

1.2. Marco de Acceso y Control

El flujo de control de acceso a dispositivos USB está gobernado por el PoLP:

1. **Regla por Defecto (Hard Deny):** Denegar acceso de escritura a **todos** los dispositivos de almacenamiento extraíble.
2. **Mecanismo de Excepción:** La excepción se implementa exclusivamente a nivel de **Grupo de Seguridad** de Active Directory, no a nivel de usuario individual (para facilitar la gestión y auditoría).

Flujo de Aprobación de Excepción (Proceso de Negocio):

1. **Solicitud:** Manager del empleado envía una solicitud justificada al CISO y al equipo de TI (Ticketing System).
2. **Justificación:** El rol del empleado debe requerir explícitamente la transferencia de datos (ej. un auditor de hardware, un ingeniero de campo).
3. **Implementación de TI:** Se agrega al usuario al Grupo de Seguridad **GRP_DLP_USB_EXCEPCION**.

Parte 2: Implementación y Comandos Ejecutados en la VM Windows

2.1. Implementación de la Restricción Global (Método 1: Registry)

Este método se utilizó para una prueba de concepto inicial, estableciendo una restricción de Denegación de Escritura a nivel de la máquina local.

Comandos de Consola (Ejecutamos como Administrador):

1. **Acceso al Editor del Registro:**
   regedit

2. Navegación a la Ruta de Control de Dispositivos:

Ruta navegada: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

3. Creación de la Clave (si no existe):
   Si la clave StorageDevicePolicies no existe, debe crearse manualmente:
   `Control > Nuevo > Clave > Nombrar: StorageDevicePolicies`

4. Creación del Valor WriteProtect:
   Dentro de la clave StorageDevicePolicies:
   `Nuevo > Valor de DWORD (32 bits) > Nombrar: WriteProtect`

5. Activación de la Protección de Escritura:
   Se establece el valor de WriteProtect a 1:
   `WriteProtect > Cambiar Valor de Datos a: 1`

   `(Valor: 1 = Habilitado, 0 = Deshabilitado)`

Efecto: Al configurar WriteProtect = 1, la VM interpreta que todos los dispositivos de almacenamiento extraíble conectados deben ser montados en modo de "solo lectura" (*Read-Only*) para todos los usuarios del sistema.

2.2. Validación de la Restricción

1. **Preparación:** Se crea un usuario sin privilegios.
   `net user usuario_regular Contrasena123! /add`

2. **Prueba:** Se inicia sesión con usuario_regular. Se inserta un USB y se intenta copiar un archivo (ej. documento.txt).
3. **Resultado Esperado y Obtenido:** El sistema operativo devuelve un error de acceso, como: **"El disco está protegido contra escritura. Quite la protección contra escritura o use otro disco."**
4. **Conclusión:** La restricción de Denegación de Escritura es efectiva para el usuario regular, pero no permite la excepción.

2.3. Investigación y Solución del Desafío del Menor Privilegio (Método 2: GPO)

El método de regedit es insuficiente porque bloquea a todos los usuarios, incluyendo a los administradores. La solución correcta para la granularidad (PoLP) debe aplicarse a nivel de identidad del usuario o grupo, lo que se logra con las Políticas de Grupo (GPO).

2.3.1. Pasos de la Investigación (Flujo del gpedit.msc)

1. **Acceso al Editor de Política de Grupo Local:**
   `gpedit.msc`

2. Navegación a la Política Requerida:

Ruta de la Política:
`Configuración del equipo > Plantillas administrativas > Sistema > Acceso a almacenamiento extraíble`

3. Configuración de la Denegación por Defecto (Regla Universal):
   Se establece la regla de negación principal:
   - **Política:** Discos extraíbles: Denegar acceso de escritura
   - **Acción:** Se establece a **Habilitada**.
   - **Efecto:** Esta directiva, al estar en la configuración del equipo, establece la restricción a nivel del dispositivo, pero **puede ser anulada por filtros de seguridad** en un entorno de dominio.
4. Implementación de Excepción Granular (Active Directory Requerido):
   Para una excepción por usuario/grupo, se requiere la consola de Administración de Políticas de Grupo (GPMC) en un Controlador de Dominio, no solo gpedit.msc.
   - **Herramienta de Solución: Filtro de Seguridad de Políticas de Grupo (GPO Security Filtering)**.
   - **Mecanismo Detallado:**
     1. **Creación de GPO:** Se crea una GPO llamada `DLP_Denegar_USB_Escritura` y se vincula a la Unidad Organizativa (OU) donde residen los equipos.
     2. **Política Interna:** Dentro de esta GPO, la política Discos extraíbles: Denegar acceso de escritura se configura como **Habilitada**.
     3. **Configuración del Filtro (PoLP):**
        - **Usuarios Afectados (Filtro por Defecto):** La GPO se aplica inicialmente a **Usuarios autenticados** (lo que incluye a todos los empleados).
        - **Configuración de Exclusión (La Excepción):** Se crea un grupo de seguridad en Active Directory llamado **GRP_DLP_USB_EXCEPCION** (Ej. Auditores de Campo). Este grupo se agrega a la sección de **Delegación** de la GPO con el permiso de **Denegar Aplicación de la Política**.
        - **Comando de actualización (en la VM/Equipo Cliente):**
          gpupdate /force

          (Necesario para aplicar los cambios de política inmediatamente.)

2.3.2. Validación Teórica de la Excepción

Usuario/Grupo	Membresía	Aplicación de GPO	Resultado de Escritura USB	Principio PoLP
usuario_regular	No es miembro de GRP_DLP_USB_EXCEPCION.	Recibe la GPO DLP_Denegar_USB_Escritura.	**DENY (Bloqueado)**	Cumplido (Menor Privilegio)

usuario_administrador	Es miembro de GRP_DLP_USB_EXCEPCION.	El filtro de seguridad DENIEGA la aplicación de la GPO.	**ALLOW (Permitido)**	Cumplido (Acceso Necesario)

2.3.3. Conclusión Final

La implementación del Principio del Menor Privilegio en políticas de control de USB requiere que la protección se mueva del **nivel del registro del sistema** (que es global) a un **nivel de identidad de grupo/usuario** mediante las **Políticas de Grupo de Active Directory** y el uso avanzado de **Filtrado de Seguridad** (Exclusión) para permitir la excepción justificada.