Políticas de DLP

Introducción a DLP

Es un conjunto de herramientas y procesos diseñados para detectar y prevenir el uso y transmisión no autorizados de información sensible. DLP es crucial en el panorama digital actual por varias razones:

1. **Protección de Datos Sensibles**: DLP ayuda a las organizaciones a salvaguardar su activo más valioso - la información.
2. **Cumplimiento**: Muchas industrias están sujetas a regulaciones que requieren la protección de tipos específicos de datos.
3. **Gestión de la Reputación**: Las filtraciones de datos pueden dañar severamente la reputación de una organización y la confianza del cliente.
4. **Mitigación de Amenazas Internas**: DLP puede ayudar a prevenir fugas de datos tanto accidentales como intencionales por parte de los empleados.

Clasificación de datos

- **Información de identificación personal (IIP):** La IIP engloba cualquier dato que distinga o rastree la identidad de un individuo, como el nombre, los números de la seguridad social, la dirección de correo electrónico o los números de teléfono.
- **Información financiera:** Detalles relacionados con cuentas bancarias, tarjetas de crédito u otras cuentas financieras.
- **Información sanitaria:** Esto incluye historiales médicos, datos del seguro médico u otra información personal relacionada con la salud.
- **Información comercial confidencial:** Datos comerciales confidenciales como secretos comerciales, datos de propiedad intelectual, información operativa o estratégica.
- **Datos de alto riesgo:** Información que, si se difunde, podría tener consecuencias graves y adversas, como el robo de identidad, el fraude o incluso incidentes de seguridad.

Acceso y Control

1. **Política de "Denegación por Defecto:** Todo acceso está prohibido a menos que sea explícitamente concedido.
2. **Acceso Basado en Roles:** Se crean roles basados en las funciones laborales ("Analista Financiero", "Agente de Soporte Técnico", "Desarrollador").
3. **Acceso Temporal:** Para tareas de alto privilegio (por ejemplo acceso de administrador a un servidor de producción), los permisos no se otorgan de forma permanente.

4. **Segregación de Funciones:** Ninguna persona debe tener el control total sobre un proceso crítico (por ejemplo, la persona que aprueba un pago no puede ser la misma que lo ejecuta).

Roles y Responsabilidades en la Revisión

- **Usuario Final:** El empleado que solicita el acceso. Es responsable de justificar la necesidad del negocio.
- **Jefe de Departamento:** Primera línea de aprobación. Valida que la solicitud del usuario se alinea con sus responsabilidades y objetivos del equipo.
- **Propietario del Sistema:** Es el responsable final del recurso (por ejemplo, el director de Finanzas es el propietario del sistema). Da la aprobación final, ya que es el máximo responsable de la seguridad de esa información.
- **Equipo de TI:** Implementa el cambio de permisos una vez aprobado. No aprueba, solo ejecuta y verifica. También es responsable de generar los informes para las revisiones periódicas.
- **Auditoría Interna:** Revisa periódicamente que el proceso de revisión se esté llevando a cabo correctamente y que los registros de auditoría sean coherentes.

Monitoreo y auditoria

Monitoreo de red y correo electrónico:

- Monitorear la transferencia de un volumen inusualmente alto de datos desde la red interna hacia destinos externos en un corto período de tiempo.
- Detectar el envío de correos electrónicos con datos clasificados como "Confidencial" o "Restringido" a dominios de correo gratuitos (gmail.com, outlook.com, etc.)

Monitoreo de estaciones de trabajo / endpoints:

- Monitorear y controlar la transferencia de archivos clasificados a dispositivos de almacenamiento extraíbles.
- Detectar un posible intento de un usuario de acceder a información para la cual no tiene permisos.

Monitoreo de base de datos:

- Monitorear el acceso a las bases de datos o carpetas más críticas de la empresa (por ejemplo, base de datos de clientes, código fuente) en horarios no habituales.

Auditorias

1. **Frecuencia:**
    - **Auditorías Semanales:** Revisión de alertas de alta y crítica severidad de la semana anterior, y revisión de los logs de acceso de administradores.
    - **Auditorías Mensuales:** Revisión de patrones de acceso, informes de DLP (intentos bloqueados, datos más accedidos) y excepciones de políticas concedidas.

- **Auditorías Trimestrales:** Coinciden con la recertificación de permisos. Se audita que los accesos coincidan con los permisos aprobados.

2. **Responsables:**
    - **Analista de Ciberseguridad:** Realiza las auditorías operativas (semanales, mensuales).
    - **Oficial de Cumplimiento / Auditor Interno:** Revisa los resultados de las auditorías y se asegura de que el proceso se siga correctamente, especialmente para cumplir con normativas (GDPR, PCI-DSS).
3. **Procedimiento:**
    - Utilizar los dashboards del SIEM para visualizar tendencias y anomalías.
    - Extraer informes específicos de la consola de DLP (ej. "Top 10 usuarios que activaron políticas de DLP").
    - Revisar los registros de acceso a sistemas críticos, buscando accesos no justificados.
    - Documentar los hallazgos y crear un plan de acción para cualquier desviación encontrada (por ejemplo, "Revocar permiso X al usuario Y", "Ajustar la regla M2 para reducir falsos positivos").

Prevención de filtraciones

Como método preventivo se utilizarán distintos tipos de cifrados:

1. *Cifrado de disco completo:* todos los portátiles y estaciones de trabajo de la empresa deben tener el cifrado de disco completo activado de forma obligatoria.
2. *Cifrado de base de datos:* todas las bases de datos que contengan información PII (Información de Identificación Personal) o datos clasificados como "Restringido" deben tener el cifrado activado.
3. *Cifrado en la nube:* todos los datos almacenados en servicios en la nube (AWS S3, Azure Blob Storage, OneDrive) deben estar cifrados en el lado del servidor.
4. *DLP de descubrimiento:* se realizarán escaneos automáticos y periódicos en todos los repositorios de archivos (servidores, SharePoint, OneDrive) para identificar datos sensibles que no estén en su lugar o que carezcan de la protección adecuada.
5. *DLP de Red y Correo Electrónico:* se inspeccionará todo el tráfico de correo electrónico y web saliente para detectar y bloquear la exfiltración de datos sensibles.

Educación y concientización

- Se realizarán jornadas interactivas de capacitación sobre la importancia de ser conscientes en el uso y manejo de datos sensibles, haciendo hincapié en los riesgos personales y empresariales que suponen la filtración o perdida de dichos datos.
- Las capacitaciones serán personalizadas para los empleados de cada área, ya que no todos los empleados manejan los mismos tipos de datos.

- Al cabo de un tiempo determinado dicha capacitación deberá ser renovada realizándose nuevamente.
- Se implementarán canales de información para que los empleados cuenten con una fuente de consulta inmediata para evacuar cualquier tipo de duda que se pueda generar en el momento.