Data Loss Prevention (DLP) Policies for external devices

Introducción al DLP: Data Loss Prevention.

El Data Loss Prevention (DLP) se puede definir como el conjunto de procedimientos, estrategias, tácticas y herramientas establecidos y orquestados por una organización para evitar la pérdida (o la fuga) de información confidencial o el acceso no autorizado a información (que no debería ser divulgada). En consecuencia, el DLP está orientado a la protección de datos sensibles, los cuales pueden ser de carácter personal, financiera y relativos a derechos de propiedad intelectual personal o de la organización. Si dicha información compromete la confidencialidad, la disponibilidad, la integridad o la reputación de dicha organización, la organización queda afectada. Tener una política de DLP en una organización, resulta esencial precisamente para proteger datos sensibles de una potencial fuga, -ya sea de forma accidental o a propósito-, y también permite proteger la organización contra el acceso no autorizado y garantizar que la misma cumple con las normativas de protección de datos y de privacidad.

Clasificación de Datos.

Con el fin de efectivamente gestionar la información, la organización debe clasificar los datos según un cierto nivel de sensibilidad, tal que se puede hacer para poder aplicar las medidas de protección adecuadas en cada tipo de dato así como garantizar que sólo las personas autorizadas puedan acceder a aquellos datos más sensibles. Por lo tanto, la política de clasificación de datos se encuentra definida de la siguiente forma:

Datos Públicos: aquellos que no contienen información confidencial o sensible y que pueden ser compartidos sin temer que se produzca algún tipo de daño potencial a nadie, es decir, que pueden ser compartidos libremente con cualquier persona, estando dentro o fuera de la organización. Ejemplos de estos datos pueden ser comunicados de prensa, materiales de marketing, y en general aquello que pueda ser accesible a cualquier persona fuera de la organización.

Datos Internos: aquellos que no deben ser compartidos públicamente, pero cuya posible divulgación a personas dentro de la organización no causaría un gran daño. Estos pueden incluir documentos internos de trabajo, políticas generales de la empresa, y otra información de tipo administrativo.

Datos Sensibles

Son datos que, si se divulgaban o exponían sin la debida autorización, podrían ocasionar un daño severo a la compañía, a los empleados o a los clientes. Se incluirían los datos personales identificativos (PII), historiales financieros, propiedad intelectual, historial médico o cualquier otro dato que fuese esencial para el negocio.

Acceso y Control.

Siguiendo el principio del menor privilegio, se restringirá el acceso a los datos para tratar adecuadamente el nivel de sensibilidad. El acceso a ciertos datos debe restringirse a los empleados que requieran el acceso a estos datos para poder llevar a cabo funciones específicas. El proceso de aprobación de acceso debe ser revisado periódicamente para garantizar que los permisos concedidos siguen siendo adecuados.

Políticas de acceso

El acceso a los datos sensibles estará controlado mediante el uso de autenticación potente, con permisos claramente definidos. Cada empleado debe tener acceso a los datos requeridos para poder llevar a cabo el papel específico que desempeñan en la organización.

Flujo de revisión de permisos

La revisión de permisos se realizará de forma semestral por un equipo de seguridad, compuesto por miembros del departamento de TI y de seguridad de la información, que se encargarán de que los accesos están en consonancia con las necesidades actuales de la organización, y que no existen accesos no autorizados.

Monitoreo y Auditoría

Para garantizar la protección de los datos sensibles, será necesario si o si monitorear y auditar el uso de estos datos. Las reglas de monitoreo de los datos sensibles deben incluir la vigilancia de cualquier actividad inusual o no autorizada, como acceso a datos sensibles

por parte de usuarios no autorizados, traslados de datos desde y hacia la red corporativa o el uso de dispositivos de almacenamiento externos.

Herramientas de Monitoreo y Auditoría

Se emplearán soluciones SIEM (Gestión de Información y Eventos de Seguridad) y herramientas especializadas de DLP (Prevención de Pérdida de Datos) para supervisar el uso de información crítica. Estas tecnologías son capaces de identificar patrones inusuales en el acceso a datos y enviar alertas en tiempo real ante posibles incidentes de seguridad.

Auditorías Periódicas

Se implementarán auditorías regulares, tanto internas como externas, para garantizar el cumplimiento de las políticas de seguridad establecidas y para evaluar la efectividad de las estrategias adoptadas.

Prevención de Filtraciones

Las filtraciones de información sensible pueden ocurrir debido a errores humanos, vulnerabilidades en la seguridad o intenciones maliciosas. Para mitigar estos riesgos, se tomarán las siguientes medidas:

Cifrado de Datos

Todos los datos sensibles, tanto en reposo como en tránsito, serán protegidos a través de algoritmos de cifrado avanzados, asegurando que la información no sea accesible en caso de ser interceptada o robada.

Herramientas DLP

Se instaurarán herramientas de DLP para impedir la transferencia no autorizada de datos críticos fuera de la red corporativa, como el envío de correos electrónicos a destinatarios no autorizados o la transferencia a dispositivos externos.

Educación y Concientización

Una de las claves del éxito en cualquier estrategia de seguridad es la formación continua de los empleados sobre los riesgos de pérdida de datos y las mejores prácticas para la protección de información sensible.

Capacitación Anual

Se llevará a cabo un programa de capacitación anual obligatoria sobre seguridad de datos para todo el personal. Esta formación abarcará temas como el reconocimiento de correos electrónicos de phishing, las mejores prácticas en el manejo de contraseñas y la relevancia del cifrado de datos.

Campañas de Concientización

Se implementarán campañas regulares para recordar a los empleados las políticas de seguridad vigentes, los riesgos que conlleva el manejo de datos sensibles y cómo identificar amenazas potenciales.

Se ingreso al editor de políticas de grupo (gpedit.msc), se negaron los accesos de lectura de usb, esto para que cuando alguna perona quiera introducir una UBS, se le niegue el acceso a la misma.