Implementa Políticas de Seguridad DLP a dispositivos de almacenamiento externo

1.Data Loss Prevention

El Data Loss Prevention (DLP), o Prevención de Pérdida de Datos, es un conjunto de tecnologías, políticas y procesos diseñados para proteger la información confidencial dentro de una organización. Su objetivo principal es evitar que los datos sensibles sean accedidos, divulgados, modificados o eliminados de manera no autorizada, ya sea por accidente o de forma intencional. Es una herramienta esencial para las empresas que buscan mantener la confidencialidad y la integridad de su información más valiosa.

El DLP no solo actúa como una capa de defensa contra amenazas externas, sino que también controla el flujo de información dentro de la propia organización. Permite monitorizar y bloquear acciones como la transferencia de datos sensibles a través de correos electrónicos, dispositivos externos, aplicaciones de nube o redes, y ayuda a aplicar políticas de seguridad en tiempo real para proteger la integridad de los datos.

La implementación de una solución DLP es crucial no solo para la seguridad de los datos, sino también para cumplir con las normativas de protección de datos que exigen un manejo adecuado de la información personal y confidencial, como el GDPR en Europa o la Ley de Privacidad del Consumidor de California (CCPA). Así, el DLP se presenta como una estrategia integral para reducir los riesgos, proteger los activos más importantes de la organización y garantizar la continuidad del negocio.

2.Clasificación de Datos:

Para establecer un DLP efectivo, el primer paso es conocer los datos que manejara la organización y cómo se clasificarán los mismos. Esta clasificación se hará en función de la sensibilidad de los datos:

º **Datos Públicos**: Son datos a los que cualquier persona puede acceder tanto dentro como fuera de la empresa, esto debido a que no suponen un riesgo que pueda comprometer la seguridad de la misma.

º **Datos Internos**: Son aquellos que la empresa necesita mantener dentro de su red interna, y solo pueden acceder trabajadores y personas autorizadas. Su filtración no

supondría un daño tan crítico como los datos sensibles pero sí podrían causar inconvenientes a la empresa y afectarla en menor medida.

º **Datos Sensibles**: Son datos de alto valor, cuya divulgación, modificación o eliminación tendrían un grave impacto en la organización, sus empleados o clientes. Son datos que se deben tener bajo una protección rigurosa y solo deben tener acceso personas específicas con privilegios adecuados.

3.Políticas de Control de Accesos

Las políticas de control de accesos son muy importantes en las empresas y es una de las bases de un DLP, esto debido a que si no se establecen correctamente cualquier persona podría acceder a datos a los que no debería tener acceso en un principio, lo cual supone un gran riesgo para la integridad de los mismos.

En este caso se establecerán políticas de control de acceso basadas en el principio de menor privilegio:

º Los permisos deben ser asignados basándose en los roles que se tengan dentro de la organización.

-Estándar: Acceso limitado a datos y funciones necesarias para cumplir con el trabajo

-Administradores: Acceso amplio a datos y herramientas del sistema para la gestión de procesos y tareas dentro de su área específica. Pero sin permisos innecesarios fuera de su área de trabajo.

-Usuarios de Acceso Crítico: Estos permisos sólo se otorgarán a personas con roles altos dentro de la organización, ya que tendrán acceso a información financiera, propiedad intelectual y demás datos que deben estar bajo estricta confidencialidad.

Además de establecer los permisos, se debe establecer un flujo de revisión de permisos, esto para mantener un monitoreo sobre los permisos que se han establecido y mantenerlos establecidos. Para esto se establecerán roles bien definidos de quienes se encargaran de establecer los permisos. Los roles responsables de la gestión de acceso y revisión de permisos son:

Departamento de TI:

º Es responsable de la implementación de políticas de acceso, gestión de herramientas de control de acceso y autenticación, así como realizar

auditorías de acceso periódicas y asistir en la revocación de permisos cuando sea necesario.

Departamento de Seguridad:

º Encargados de establecer las políticas de control de acceso basadas en el principio del menor privilegio y asegurar su cumplimiento en toda la organización.

Gerentes y Supervisores de Área:

Tienen la responsabilidad de revisar las solicitudes de acceso relacionadas con su equipo o área y verificar si son necesarias para el rol de cada empleado. También son los encargados de modificar los roles de acceso de un empleado en función de un cambio de área o de que abandone la empresa.

4.Monitoreo y Auditoría de Datos Sensibles

El monitoreo y auditoría de los datos sensibles que maneja la organización es esencial dentro del entorno de seguridad de cualquier organización, ya que ayuda a prevenir y mitigar cualquier actividad sospechosa que se presente. Para ello estableceremos reglas que establezcan un monitoreo exitoso:

º Monitoreo en tiempo real de accesos: Se deben monitorear y registrar todos los accesos y actividades relacionadas con los sensibles.

º Monitoreo de transferencia de datos sensibles: Toda transferencia de datos sensibles de la organización ya sea por correo electrónico, dispositivos USB, etc. Debe ser monitoreada y registrada para detectar actividades sospechosas.

º Monitoreo de uso de dispositivos y redes: Las actividades que involucren dispositivos como portátiles o USB deben ser monitoreadas en tiempo real ya que podrían usarse como un canal de fuga de datos.

º Control sobre la visualización de los datos sensibles: Los usuarios deben ser monitoreados para asegurar que solo acceden y visualizan datos sensibles cuando sea estrictamente necesario para sus funciones. Esto incluye la monitorización de accesos a bases de datos, documentos cifrados o registros de clientes.

º Monitoreo de aplicaciones específicas: Se deben monitorear las aplicaciones empresariales que gestionen datos sensibles.

Para garantizar que las reglas que hemos diseñado se cumplan, debemos determinar cuáles serán las herramientas de las que se dispondrán para la tarea de monitoreo.

SIEM: Esta es una herramienta que nos permite la recolección, correlación y análisis en tiempo real de eventos de seguridad generados por los sistemas. Estos sistemas nos permiten generar alertas, informes detallados sobre incidentes registrados y nos da la posibilidad de que ante eventos de seguridad determinados, no solo nos alerte sino que también responda ante la brecha de seguridad.

5.Prevención de Filtraciones:

Ante una brecha de seguridad, lo primero que debemos asegurarnos es que no se filtren los datos. Para ello tomaremos ciertas medidas que y la inclusión de herramientas que nos llevaran a garantizar la seguridad de los mismos:

- º Cifrado de datos en Reposo: Los datos almacenados en servidores, bases de datos, sistemas de archivos y demás, deben estar cifrados, de esta manera nos aseguramos de que ante un acceso no autorizado no puedan acceder a los datos sin la llave descifrado.

- º Cifrado en Tránsito: Nos aseguraremos de que los datos que se transmiten por la red tanto dentro de la organización como fuera, queden totalmente inutilizados sin las claves de descifrado.

- º Cifrado de Aplicaciones: Si disponemos de aplicaciones que manejen datos sensibles, estas aplicaciones deben garantizar que los datos dentro de las mismas estén protegidos, esto incluye aplicaciones tanto internas como externas.

Las herramientas de DLP se centran en evitar la fuga de datos sensibles al monitorear, identificar y bloquear su transferencia no autorizada fuera de los límites de la organización. Estas soluciones son fundamentales para prevenir filtraciones accidentales o malintencionadas.

- º Entre ellas podemos diferenciar entre herramientas de monitoreo y control de los datos en movimiento. Estas nos permiten ejercer control sobre el tráfico de los datos sensibles de la organización y si se registra algún

evento de envío de datos sospechoso, bloquean la transmisión de los mismos. (Symantec DLP, Forcepoint DLP, Digital Guardian DLP.)

º Por otro lado contamos también con herramientas que monitorean el acceso de los usuarios, esto nos agrega otra capa mas de seguridad porque podríamos prevenir cualquier intento de extracción de datos sensibles antes de que suceda, conociendo los patrones de comportamiento de los usuarios, accesos no autorizados, descargas masivas de datos, etc. (McAfee Total Protection for DLP, Forcepoint Insider Threat Protection, Vormetric Data Security Platform.)

6.Concientización del Personal

Uno de los objetivos más importantes a la hora de garantizar la seguridad de la información dentro de la organización es la concientización de los empleados a la hora de tener buenas prácticas de seguridad como creación de contraseñas seguras, almacenamiento seguro de las mismas, no apertura de correos electrónicos sospechosos, etc..

º Para la capacitación de los empleados lo primordial es hacerles entender de la importancia de la seguridad y la protección de los datos.

º Que sepan reconocer las amenazas que se pueden encontrar en la red como el phishing, el malware, la filtración de datos, etc. Y las consecuencias que puede conllevar no seguir las políticas de seguridad establecidas.

º Que conozcan las políticas de seguridad de la organización y cómo ponerlas en práctica.

º Simulacros de phishing cada cierto tiempo para saber si están aplicando las medidas de seguridad establecidas.

7.Conclusión

La correcta implementación de un DLP nos permite reducir los vectores de ataque que puedan explotar en contra de la organización, ya que nos permite implementar reglas de seguridad estrictas como y la implementación de controles de acceso basados en el principio de menor privilegios y monitoreo constante de nuestro sistema tanto interno como de aplicaciones externas. Con las herramientas adecuadas minimizamos riesgos de accesos no autorizados y pérdida de datos.