Data loss prevention (DLP) para TechCorp

Mauricio Piscitelli
9 de diciembre del 2024

La prevención de perdidas de datos (DLP) es un conjunto de herramientas y procesos diseñados para detectar y prevenir el uso y la transmision no autorizados de información sensible. Enfatiza la protección de datos sensibles al mismo tiempo que cumple con las regulaciones para mitigar las amenazas y mantener la reputación y confianza de las organizaciones.

En la organización podemos clasificar los datos sensibles en tres tipos de datos. La primera categorìa es sobre los datos públicos, la segunda categoría son los datos sensibles y por último los datos internos.

En los **datos públicos** se encontraron los siguientes datos:

-**Correo electrónico de la organización o de areas implicadas en la atención al cliente.**
-**Nombre y apellidos de los empleados.**
-**Dirección de la organización.**

En los **datos sensible** se encontraron los siguientes datos:

-**Nóminas.**
-**Informes financieros de estados.**
-**Datos de los clientes.**

En los **datos internos** se encontraron los siguientes datos:

-Estrategias de negocio o mercado.
-Informes de desempeño de los empleados.
-Información y documentación de los proyectos en cursos.

La prioridad es proteger estos datos para que no ocurran ninguna filtración de información, por lo que se hara uso del principio del menor privilegio.

Las políticas que se implementaran se detallan a continuación:

-**Control de acceso basado en roles(RBAC):** Se asignara permisos basado en los roles o grupos dentro de la organización. En este sentido, los de recursos humanos no podrán acceder a información financiera y vice-versa.

-**Politíca de no acceso por defecto:** Los usuarios y sistemas no pueden otorgar acceso por defecto a ningún recurso. Los accesos deben ser segun la necesidad y contexto, siempre y cuando sea absolutamente necesario.

-**Auditoría y monitoreo:** Los usuarios con privilegios elevados serán monitoreados constantemente por el equipo de IT a cargo de la seguridad informática DLP, con ayuda de sistemas EDR y SIEM.

-**Revisión periódica de permisos.**

-Acceso minimo necesario.

Para mantener la CIA de los datos, se ejecutara un plan de monitoreo y audítoria periódicamente. El plan lo llevara el equipo de seguridad DLP, siempre que sea autorizado por el gerente de dicha area.

Durante los monitoreos se debe documentar cada actividad y debe quedar registradas, en caso de haber una excepción se debe revisar con la aprobación del gerente, se debe documentar así como comunicarlo a todos de dicha excepcion de forma clara y concisa. Se realizaran tareas de capacitación y se mantendrá bajo revisión y actualización constante.

Siempre que se encuentre un falso positivo, se debe realizar un ajuste en el plan de monitoreo para reducir la cantidad de falsos positivos.

La herramienta que se utilizará para el sistema EDR y SIEM sera **Wazuh,** gracias a esto se podrá reaccionar a tiempo ante una amenaza, así como mantener un registro de los logs y login para su posterior análisis. También **Wazuh** nos permite tener flexibilidad y escabilidad. Como seguridad adicional se aplicara un honeypot en todas las areás que contengan información sensible.

El areá de la infraestructura TI de los servidores estara siempre en una areá desmilitarizada (DMZ) y con restricción física a la que solo podrá ingresar el personal unicamente autorizado con datos biometricos.

Para la nube AWS se utilizará la herramienta de cifrado **AWS Key manangement service** y para los archivos **LUKS** con la intención de poderlo integrar con nuestras herramientas y que no tenga un alto impacto en el rendimiento de la organización.

Los controles de acceso que se implementarán será para la nube **IAM** y para el usuario **OpenLDAP.** Para la web se debe tener certificado **TLS/SSL** y debe ser **HTTPS** para un cifrado más seguro y confiable. En cuanto a la comunicación interna se utilizara el protocolo **SFTP** lo que nos asegura el cumplimiento normativo.

En caso de necesitarse conectar a la red de la organización externamente, se utilizará un VPN, como lo es **Cisco ASA** ya que posee alta confiabilidad y prevención de intrusiones.

El objetivo de este informe es realizar un plan en el que mantenga la CIA de la información en la organización, por lo que para cumplirlo cada persona que forme parte de la organización tendrá que asistir a capacitaciones,sin excepciones, en las que se explicara el riesgo, prevención y plan de acción en caso de algún ataque malintencionado. También se harán campañas por redes sociales y para los clientes, con el fin de ayudarlos a identificar posibles ataques de phishing y de estafas.