Ventajas de un enfoque de seguridad centrado en los datos

Abstract: la explosión de la colaboración, el trabajo remoto y la nube han hecho que la infraestructura IT sea cada vez más compleja y el perímetro de seguridad de la red se difumine. Cuando hay una brecha de seguridad en las defensas perimetrales, la información queda expuesta. Por todo ello, cobra cada vez más importancia la necesidad de una protección centrada en los datos, que permita protegerlos, tenerlos bajo control y auditar su uso, no sólo dentro de la organización sino allí donde estos viajen o se almacenen.

Contenido:

1. LIMITACIONES DE UN ENFOQUE DE SEGURIDAD TRADICIONAL

El fin último de las inversiones en seguridad es proteger lo más valioso de la organización: los datos, especialmente los más sensibles. Si se presta atención a cómo se producen algunas fugas o pérdidas de información en las empresas, se pueden encontrar algunos de los siguientes casos de uso:

- Un **empleado deja la organización y se lleva consigo información sensible** que cree que puede utilizar en otras compañías. El empleo de la nube, dispositivos personales o el hecho de poder trabajar en remoto hacen que sea cada vez más sencillo extraer esta información.
- Un **descuido o error humano** puede hacer que un usuario envíe información con datos sensibles al destinatario equivocado, haciendo que los datos de la organización acaben en manos no deseadas.
- Se trabaja con **socios de negocio, subcontratas y otros colaboradores que tienen acceso a información sensible** en redes y equipos no controlados. Se puede configurar de manera segura la red de la organización, pero no controlar la de un tercero, que puede ser más propensa a sufrir una brecha de seguridad.
- **Ataques dirigidos como el ransomware**, donde antes de cifrar los datos, el atacante los extrae y pide un rescate a la organización para no hacerlos públicos.

Las **defensas perimetrales como cortafuegos, detectores de intrusos y otras pasarelas de protección** perimetral están pensadas para proteger la infraestructura, redes y dispositivos internos. Sin embargo, cuando se quiere controlar el acceso a la información dentro de la entidad o cuando es enviada fuera, este tipo de protección no es suficiente.

También existen en las organizaciones medidas para intentar evitar la exfiltración de información sensible, como puede ser un **DLP (*Data Leak Prevention*)**. Sin embargo, no es fácil automatizar qué es sensible y qué no, qué debe ser bloqueado o qué tipo de información se debe dejar pasar. Muchas veces es necesario compartir información sensible con socios de negocio y bloquear la salida de la misma puede impedir procesos de negocio necesarios, aumentando la frustración de los usuarios con las herramientas de seguridad.

Por otro lado, una vez que la información ha salido de la organización, estas herramientas no pueden hacer nada para controlarla. Lo mismo sucede con herramientas tipo **CASB (*Cloud Access Security Brokers*)** que actúan como protección DLP en aplicaciones en la nube. Una vez que la documentación ha sido descargada de la nube, quedan fuera del control de la organización.

Otra técnica utilizada para proteger el acceso a la información es el **cifrado**. Sin embargo, una vez que el receptor descifra el documento, se pierde el control de la información que podrá ser copiada, reenviada, etc. sin que se pueda evitar. Además, las soluciones de cifrado tipo PGP han sido tradicionalmente complejas de utilizar por parte de los usuarios.

En definitiva, los datos son un elemento vital y aunque todas las soluciones de protección perimetral son absolutamente necesarias para proteger las redes, dispositivos y aplicaciones, cada vez es más necesario cambiar el enfoque de medidas de seguridad basadas en la infraestructura a medidas de seguridad centradas en los datos.

2. RETOS DE LOS EQUIPOS DE SEGURIDAD EN EL ÁMBITO DE LA PROTECCIÓN DE LA INFORMACIÓN

Los equipos de seguridad de las entidades se enfrentan cada vez más a retos derivados de las limitaciones presentes en un enfoque basado únicamente en la seguridad perimetral:

- **El reto de la protección en cualquier lugar:** no es suficiente con tener la información protegida en un servidor de ficheros o dentro de la red. Se debe poder mantener la protección sobre la información corporativa incluso aunque haya salido fuera del perímetro de la organización y esté en manos de un tercero.
- **El reto de la visibilidad:** existen diferentes herramientas para monitorizar el acceso a determinadas aplicaciones o dispositivos. Pero, ¿cómo se puede tener visibilidad de quién accede a los datos allí donde estén? o ¿cómo ver intentos de acceso por parte de personas que no deberían tener acceso a los datos cuando estos ya han sido enviados a un tercero o están en un equipo no controlado por la organización?

- **El reto del control:** dentro del perímetro de seguridad de la organización se puede bloquear el acceso a determinados equipos o aplicaciones por parte de usuarios internos. Pero, ¿se puede hacer lo mismo con la información corporativa distribuida fuera de la organización o fuera de las aplicaciones y que está en los equipos de los usuarios?
- **El reto del tiempo de respuesta frente a incidentes de seguridad:** cada vez se opera más rápido, generando cada vez más información sensible en formato digital, compartiéndose cada vez por más medios. La solución no es poner barreras a la agilidad del negocio, sino ser capaz de detectar cuándo la información está en riesgo y poder tomar acciones inmediatas para evitar una posible fuga.
- **El reto de la sencillez de uso por parte de los usuarios:** existe una gran diferencia en una organización entre lo que la gente puede hacer y lo que realmente hace. La seguridad es normalmente vista por los usuarios como un freno al negocio. Por eso es fundamental intentar no bloquear los flujos de trabajo normales y permitirles seguir trabajando con sus herramientas habituales, pero controlando en todo momento que el nivel de seguridad es adecuado.

3. BENEFICIOS DE UN ENFOQUE DE SEGURIDAD CENTRADO EN LOS DATOS

Un enfoque de seguridad centrado en los datos permite que los datos estén protegidos y bajo control allí donde viajen: dentro de la red corporativa, en el equipo de un colaborador externo o en casa de un empleado.

La protección forma parte del documento o fichero y le acompaña allí donde éste se desplace o almacene. Con este tipo de seguridad se pueden extender medidas de control sobre la información más allá del perímetro de seguridad de la red corporativa.

Este tipo de seguridad ofrece una protección de datos en tránsito, cuando están siendo enviados a un tercero; en reposo, cuando están almacenados en un determinado repositorio; y en uso, cuando la información está siendo consumida por un usuario.

Además, permite tener trazabilidad completa de las acciones sobre un determinado fichero: quién lo abre, si alguien lo está intentando abrir sin permisos, si alguien lo intenta abrir desde una ubicación no permitida, etc.

Este enfoque de seguridad ofrece los siguientes beneficios a una organización:

- **Evita fugas de datos derivadas de acciones inapropiadas por parte de empleados, ya sea de forma accidental o maliciosa:** la información viaja protegida y sólo los usuarios que tengan permisos sobre la misma podrán acceder a ella. Un usuario puede trabajar con la información, pero puede no tener permisos para desprotegerla.

- **Facilita la colaboración segura,** haciendo que la información se comparta con terceros protegida y bajo control. Se pueden compartir documentos confidenciales con un tercero, pero garantizar que su propietario sigue siendo el dueño de los mismos y en su caso, auditar su uso. Asimismo, en su caso puede revocar el acceso a la documentación, aunque la tenga en su equipo.
- **Ayuda al cumplimiento de regulaciones de protección de datos:** regulaciones como EU-RGPD, obligan a empresas que tengan datos personales de terceros a tenerlos controlados. Cifrándolos y auditando su uso, independientemente de dónde se encuentren, se estará consiguiendo un control superior sobre los mismos y facilitando el cumplimiento de este tipo de regulaciones.
- **Protege frente a brechas de seguridad en la red que supongan una posible exfiltración de datos:** por ejemplo, en ataques de tipo ransomware, donde se exfiltran documentos, correos electrónicos y datos internos de las entidades y se extorsiona a las mismas con la publicación de estos datos. Si los datos están protegidos y cifrados, aunque se exfiltren, el atacante no podrá utilizarlos para extorsionar con su publicación.

4. CARLA. PROTECCIÓN, CONTROL Y TRAZABILIDAD DE LOS DATOS

CARLA es una solución de protección centrada en lo datos, que permite tener la documentación sensible de las organizaciones cifrada en tránsito, en uso y en remoto, minimizando la posibilidad de fugas de datos y aumentando el control de la organización sobre la misma.

CARLA ayuda a las organizaciones a cubrir las limitaciones o retos de los equipos de seguridad a través de las siguientes características:

- **Protección que viaja con los datos:** CARLA aplica un cifrado sobre la información que le acompaña allí donde se almacene o desplace. Esta protección se mantiene también fuera del perímetro de seguridad de la red, cuando se ha compartido la documentación con un tercero.
- **Trazabilidad y visibilidad sobre los datos:** CARLA permite monitorizar el fichero desde que se protege, dejando traza de quién accede, cuándo, con qué permisos, si alguien intenta acceder sin permisos o desde una subred no permitida por la organización, sin importar que la información esté en casa de un empleado, en otro país o en equipos no controlados por la organización.
- **Control de acciones sobre el documento:** con CARLA se puede permitir que un usuario vea un documento, pero que disponga de permisos para modificarlo, imprimirlo o exportar su contenido. Se pueden también establecer permisos granulares sobre la información y decidir el nivel de control que un tercero tiene

sobre la misma. La protección es también en uso, lo que permite mantener en todo momento la propiedad sobre los datos corporativos.

- **Responder en tiempo real frente una posible fuga:** CARLA permite poner limitaciones de tiempo de acceso a documentos o revocar el acceso a los datos cuando se haya decidido que alguien no debe volver a acceder.
- **Sencillez de uso:** no se intentan bloquear las posibles vías de salida de información de la red, sino que la información saldrá protegida y bajo control, pero se puede seguir utilizando el correo electrónico, la nube u otros medios para compartir los datos.

5. CASOS DE USO DE UNA HERRAMIENTA DE SEGURIDAD CENTRADA EN LOS DATOS

En el día a día en las organizaciones se pueden encontrar diferentes situaciones donde resulta fundamental tener un control sobre los datos que vaya más allá de las defensas de protección perimetrales. Algunas de estas situaciones son:

- **Facilitar un trabajo remoto seguro:** el trabajo remoto puede suponer graves riesgos en lo que respecta a la gestión de información sensible. A través de un enfoque de seguridad centrada en los datos, el dueño de los documentos tiene la capacidad de tener trazabilidad sobre los accesos y controlar sus datos. El acceso puede ser instantáneamente revocado si se deja de trabajar con un usuario.
- **Incrementar la seguridad en la nube:** la compartición de información en la nube ha crecido exponencialmente en los últimos años. Aplicando cifrado a los datos se puede garantizar que estos están seguros tanto si se almacenan en una nube privada o pública como si el usuario los ha descargado en su equipo.
- **Salvaguardar documentación financiera o legal:** dos de los departamentos de las organizaciones que más información sensible gestionan son el financiero y legal. El riesgo no solo se encuentra fuera de la organización, sino también se ha de tener en cuenta que a esta información se pueda acceder internamente por parte de usuarios malintencionados. Resulta fundamental mantenerse a salvo de accesos indebidos y trazando cualquier acceso incluso por parte del personal IT.
- **Proteger información de Dirección, recursos humanos, datos técnicos o propiedad intelectual:** resulta crítico controlar quién puede tener acceso a esta información, con qué permisos, desde qué redes y se auditen en todo momento posibles accesos indebidos.
- **Cumplimiento de regulaciones:** las organizaciones se encuentran sujetas a diferentes regulaciones que hacen necesario extremar las precauciones sobre determinados datos. En el caso de empresas y organizaciones que operan en el ámbito de la Unión Europea, es necesario mantener bajo control la gestión de los

datos personales de ciudadanos, especialmente datos de ciertas categorías como los datos médicos. Estas regulaciones recomiendan normalmente el cifrado como una técnica eficiente de protección, pero si además se pueden aplicar controles de acceso, revocación y auditoría, se estará mejorando de forma sustancial la seguridad con la que se gestiona internamente este tipo de información.

- **Extender la seguridad proporcionada por un DLP o CASB:** este tipo de herramientas permite bloquear la salida de información sensible de la organización vía correo electrónico y otros medios. Complementar un DLP o CASB con seguridad centrada en los datos, permite extender el control de la información sensible más allá de la red corporativa, aunque la información haya sido descargada de una determinada nube.
- **Protegerse en las comunicaciones o colaboración con subcontratas:** en muchos entornos, en especial en el ámbito de industria o fabricación, se trabaja con determinados proveedores o subcontratas que ayudan en el desarrollo de producto. Si se comparte la documentación o ficheros sensibles con ellos de forma que se pueda controlar quién los abre, hasta cuándo y revocar su uso, se estará ampliando el nivel de seguridad en la colaboración.
- **Protección de información clasificada o acceso restringido:** en función del grado de clasificación de la información, el tratamiento que se debe dar a esta información está regulado por procedimientos operativos de seguridad. Se trata de trasladar el concepto de etiqueta de seguridad del mundo físico al virtual haciendo que cada tipo de información pueda ser abierta por un determinado colectivo de usuarios y con permisos limitados.

6. LA SEGURIDAD CENTRADA EN LOS DATOS EN UN MODELO ZERO-TRUST O SASE

El modelo de seguridad *Zero-Trust*, se basa en la premisa de que no se puede garantizar que un usuario interno es “confiable”. Por tanto, se debe:

- **Asegurar que los recursos son accedidos de forma segura con independencia de su ubicación:** se deben proteger los datos en el interior de la entidad de la misma forma que si estuviesen fuera en internet. Toda conexión a los datos es no confiable hasta que no se demuestre lo contrario, independientemente desde dónde se haga.
- **Adoptar la estrategia del “modelo de acceso de menor privilegio” y forzar controles de acceso estrictos:** se debe dar acceso a una persona sólo a los recursos que necesita para realizar su trabajo e impedir el acceso al resto. Es necesario controlar el acceso a la información sensible, controlando la identidad, el dispositivo, aplicación y en definitiva el contexto desde el que se intenta acceder.

- **Inspeccionar y registrar todo:** se debe inspeccionar la actividad no sólo en el acceso a la red sino también en el interior, intentando identificar comportamientos anómalos. Esto permite lanzar el mensaje a los posibles atacantes de que se les está monitorizando, para que desistan en sus intenciones.

El modelo *Secure Access Service Edge (SASE)* es un marco de seguridad para permitir la adopción segura y rápida de la nube, y ayudar a garantizar que tanto los usuarios como los dispositivos tengan acceso seguro en la nube a aplicaciones, datos y servicios en cualquier lugar y en cualquier momento. A medida que las organizaciones buscan acelerar el crecimiento mediante el uso de la nube, se utilizan más datos, usuarios, dispositivos, aplicaciones y servicios fuera de la operativa tradicional, lo que significa que el perímetro ya no es una ubicación definida, sino una ubicación dinámica en función de las necesidades de servicios en la nube.

Este nuevo **perímetro dinámico** cambia la forma en que las organizaciones deben abordar la seguridad y la gestión de riesgos. Agrega complejidad y dificulta el control, debido a que los usuarios, los dispositivos y los datos se crean y almacenan prácticamente en cualquier lugar.

Una estrategia de seguridad centrada en los datos está completamente alineada con estos modelos:

- Las políticas de seguridad se extienden más allá del perímetro físico de la red y permiten aplicar un “perímetro de seguridad dinámico” sobre los datos.
- En cada acceso se puede realizar un control de quién intenta acceder al documento y permitir o no en función de los privilegios otorgados.
- El control de acceso es estricto, permitiendo el acceso sólo con permisos de lectura, por ejemplo, pero sin dar la posibilidad de imprimirlo o desprotegerlo.
- Se auditan y monitorizan los accesos y los intentos de accesos bloqueados.
- Se puede cambiar el control de acceso de forma dinámica para revocar permisos o ampliarlos respecto a los asignados originalmente.

7. RESUMEN

El enfoque de una herramienta de seguridad centrada en los datos permite que la información corporativa viaje protegida y bajo control en todo momento. De esta forma, se puede tener una trazabilidad completa de acciones sobre la misma.

La protección se extiende más allá del perímetro de la red y permite aplicar controles efectivos sobre información clasificada. En el mundo físico, un documento puede llevar la etiqueta de “USO OFICIAL” y se establecen determinados procesos internos de gestión del mismo. En el mundo virtual, CARLA puede aplicar control sobre documentos

virtuales de “USO OFICIAL” que limitan quién puede acceder, con qué permisos y auditar su uso.

Una herramienta como CARLA permite tener un control virtual en el equipo de otra persona. Es decir, tiene los datos físicamente en su equipo, pero será la organización la que determine las reglas de acceso a esos datos, los permisos y hasta cuando se autoriza el acceso a los mismos.

De esta forma, se puede establecer una colaboración segura con terceros, prevenir posibles fugas de datos, mejorar el cumplimiento de regulaciones y mejorar la protección frente a una posible brecha de seguridad en la red.