NOTA DE PRENSA
09 / 10 / 2020

Colaboración segura con SealPath dentro y fuera de las organizaciones

> El boom del teletrabajo y la colaboración con los partners hacen que el perímetro de seguridad deba ir más allá de las fronteras de la organización

Madrid, 9 de octubre de 2020.- La pandemia por COVID-19 ha acelerado la transformación digital por parte de las empresas. Antes sólo el 10% de las organizaciones teletrabajaban –aunque en el 50% de los casos esta modalidad de trabajo en remoto era factible–. Ahora el 74% de las empresas han implementado el teletrabajo, ya sea en su totalidad o parcialmente.

“Hay quien considera que la transformación digital debe venir de la mano del CEO o del CTO de la compañía, sin embargo, en este caso, la COVID-19 nos ha impulsado a ser más digitales. El hogar es ahora bimodal, es decir, ya no es sólo un lugar de descanso y diversión, sino que también se ha convertido en un entorno para el trabajo. En casa, tenemos la capacidad para desarrollar todo lo que antes hacíamos en la oficina”, comenta Luis Miguel Gilpérez, Asesor de Consejo de Administración de SealPath y ex Directivo de Telefónica.

Las redes de comunicación, la fibra o el 5G son elementos que han hecho posible esta transformación digital acelerada. A pesar de ello, según apunta Gilpérez, queda mucho camino por recorrer. “Necesitamos una administración mucho más digital, así como potenciar el teletrabajo en todas las organizaciones de la sociedad, no sólo en las grandes empresas, tenemos que extenderlo a cualquier otro sector como puede ser la educación, la sanidad o la industria. Y, en este sentido, la ciberseguridad es un elemento clave”, apunta el directivo.

Según el World Economic Forum, los riesgos que más preocupan a las organizaciones son en tercer lugar los ciberataques. Durante la pandemia se ha incrementado el número de ataques, sobre todo dirigidos a hospitales, el sector financiero y tributario. “Nuestros hábitos han cambiado, estamos en

un entorno con mayor colaboración, además tenemos acceso a información crítica fuera de la red de la compañía. Por ello, es importante proteger el hogar y a los miembros de nuestro entorno ya que en casa hay mayor probabilidad de ser atacados al estar menos protegidos. No podemos desproteger el bien más preciado que tenemos: nuestros datos", afirma Gilpérez.

¿Cómo ha cambiado la forma de securizar las organizaciones?

La COVID-19 ha hecho que las organizaciones cambien sus partidas presupuestarias para adaptarse a la nueva situación, ya que la mayoría de ellas no estaba preparada para teletrabajar. Por ello, la prioridad en un primer momento de los CISOS o responsables de ciberseguridad fue dotar a todos los empleados de las herramientas adecuadas para un entorno de teletrabajo, dejando para una segunda fase la ciberseguridad.

"La disponibilidad de poder trabajar desde casa, de acceder a las aplicaciones y de no notar la diferencia con el puesto de trabajo fueron los principales retos de los CISOS. La COVID-19 ha acelerado la transformación digital de las empresas a marchas forzadas. La colaboración antes no era tan intensa como ahora y, como consecuencia, la información puede estar en cualquier sitio, cualquier lugar o cualquier dispositivo. A raíz de esto se abren diversos agujeros de seguridad en torno a la empresa y a la persona", señala Javier Modúbar, CEO de Ingecom.

En este sentido, el perímetro de seguridad que conocíamos hasta ahora se ha diluido. Actualmente, lo que importa es proteger al ser humano, al dispositivo y al dato. En el caso del ser humano, la ciberseguridad está evolucionando hacia el concepto de Zero Trust. "El usuario piensa que al estar en casa se encuentra en un entorno más seguro, pero posiblemente sea más vulnerable. Por ello, es imprescindible dotar de tecnología el entorno de la persona", explica Modúbar.

Entre otras herramientas, el directivo de Ingecom recomienda implementar tecnologías de concienciación y aprendizaje para evitar posibles amenazas ya que el principal vector de ataque es el correo electrónico. "Un usuario que abre un phishing crea un agujero de seguridad en su equipo, ya sea personal o corporativo. Por este motivo, es importante no sólo poner barreras de securización sino también concienciar a los trabajadores de los riesgos de la red".

Otras tecnologías que se deberían aplicar para proteger al usuario son las herramientas de gestión de identidad (IAM), que permiten establecer quién puede acceder a una determinada información, así como soluciones de análisis de comportamiento para detectar posibles amenazas. "Es imprescindible combinar varias tecnologías para hacer a la persona más segura ya que a veces los propios usuarios están comprometidos sin saberlo".

En el caso de los dispositivos, la ciberseguridad se basa fundamentalmente en tecnologías de EDR, software de gestión de vulnerabilidades o gestión de contraseñas, ya que el fin último del atacante es acceder a los datos más sensibles de las organizaciones para extorsionarlas. “Contar con tecnología de DLP es importante, pero cuando la información se comparte con terceros o sale de la organización, necesitamos herramientas de IRM, como SealPath, que permitan controlar la información como última barrera. Además, utilizar tecnología de clasificación de información agiliza esta tarea”, cuenta Modúbar.

> La información, el activo más valioso de las organizaciones

Hoy en día el dato puede estar en cualquier sitio, por ello es necesario protegerlo ya que es uno de los activos más valiosos de las organizaciones. En este aspecto, SealPath es una solución de protección y control de información que permite a las empresas mantener a salvo los datos más sensibles, no sólo dentro de la compañía sino también en entornos de colaboración.

“Desde SealPath ofrecemos una modelo de transferencia de información segura en el que se evita el anonimato, se identifica al emisor y se cifra de extremo a extremo. Además, es posible una compartición segura, con permisos por usuario, tracking de accesos y posibilidad de revocación. Y, por último, una colaboración segura que permite la edición y colaboración en tiempo real”, argumenta Luis Ángel del Valle, CEO de SealPath.

Asimismo, esta solución permite crear un modelo de protección basada en círculos de confianza para evitar fugas de información. Por otra parte, la herramienta es muy fácil de utilizar y se integra con todas las aplicaciones corporativas. El usuario puede proteger la información fácilmente y seleccionar los diferentes permisos (editar, copiar y pegar, desproteger la información y reenviarla, entre otros aspectos). De igual modo, es posible comprobar quién ha abierto el documento y qué ha hecho con él.

“Incluso es posible automatizar la protección. Por ejemplo, cuando se envía un correo electrónico que contiene números de tarjeta bancaria, se puede proteger automáticamente sin que tenga que intervenir el usuario. Nuestra estrategia es proteger la información en cualquier formato y lugar, en un modelo multiplataforma y sin agentes”, concluye el directivo.

SealPath está presente en más de 20 países y trabaja con el canal a través de Ingecom tanto en Iberia como en Italia. Asimismo, cuenta con una gran base de clientes de sectores financieros y de energía, entre otros, y se integra con otros fabricantes de seguridad.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net