NOTA DE PRENSA
10 / 07 / 2020

SealPath ayuda a proteger los datos en este período de nueva normalidad

> Durante la Covid-19, un nutrido número de organizaciones ha sido testigo de cómo la pandemia llevaba aparejados no sólo problemas económicos, sino también un aumento masivo de ciberataques

La mayor parte de las empresas han visto como aumentaban sensiblemente los ciberataques a nivel mundial durante la pandemia de coronavirus. Según una encuesta realizada por PwC a CISOs y CIOs respecto al entorno de ciberseguridad post-Covid, los ciberataques se han incrementado en marzo y abril de este año, esperándose picos de intrusiones durante los próximos seis meses. A finales de febrero, sólo los ataques de phishing habían aumentado más de un 600% y hemos visto como surgían brotes de suplantación de identidad a medida que el coronavirus se extendía a nivel mundial.

Durante la Covid-19, un nutrido número de organizaciones ha sido testigo de cómo la pandemia llevaba aparejados no sólo problemas económicos, sino también un aumento masivo de ciberataques. Y después del período más crítico del coronavirus, se han prolongado los incidentes de ciberseguridad; en mayo, más de 150 organizaciones a nivel global han visto sus datos sensibles publicados y han sido extorsionadas para evitar la publicación de su información crítica.

Ante la nueva situación, las corporaciones han realizado a marchas forzadas una rápida transformación en su modelo de trabajo, apostando por el teletrabajo y desplazando a su fuerza laboral más allá del tradicional perímetro de seguridad de la red corporativa.

Luis Miguel Gilpérez, Asesor de Consejo de Administración de SealPath y ex Directivo de Telefónica, comenta que: “Estamos ante una nueva normalidad. Durante el período de confinamiento hemos cambiado nuestros hábitos, pasando a realizar el trabajo desde casa y demostrando que se podía hacer. Hemos dado el salto para ser más digitales, no solo como personas, sino como empleados y

como sociedad en general. Podría decirse que la pandemia nos ha abocado a un escenario en el que hemos vivido una prueba piloto de cambio basado en lo digital a todos los niveles que nos va a tocar afrontar en los próximos meses. La Covid nos ha enseñado que la transformación digital no es una opción; a partir de ahora, o eres digital o no te integrarás en la nueva sociedad laboral".

Gilpérez asegura que la actual situación "es solo la punta del iceberg" de lo que viene por delante, "nos vamos a enfrentar a una transformación digital mucho más potente. Tenemos un nuevo reto como sociedad y debemos aprovechar que España tiene una gran red de comunicaciones y somo el país de Europa con más fibra. El hogar en estos momentos es bimodal. Por un lado, se ha convertido en nuestra oficina y, por otra parte, es nuestro lugar de ocio y descanso; los dos modelos hacen que la forma de actuar sea diferente: vamos a estar menos en la calle y vamos a apostar por momentos de entretenimiento basados en dispositivos digitales".

Aun así, nos queda mucho camino por recorrer, especialmente en el entorno de la Administración, el teletrabajo en pymes y la ciberseguridad en general. "El confinamiento ha favorecido un campo de trabajo más abierto y, dejadme decirlo, más permisivo, con lo cual, tenemos que ser mucho más seguros. Debemos incidir en potenciar la formación en ciberseguridad de los usuarios para garantizar la seguridad a todos los niveles", advierte Gilpérez.

Durante la pandemia, se han incrementado los ciberataques, a pesar de que contamos con herramientas de seguridad suficientes para hacerles frente. La cuestión ha sido que no todo el mundo dispone de los recursos de seguridad, por desconocimiento o por falta de inversión en ellos. El teletrabajo ha demostrado que se puede trabajar en remoto, que usamos más dispositivos que nunca, pero que ha aumentado el riesgo de ciberataques. También ha revelado otra tendencia, y es que los datos y las aplicaciones están moviéndose vertiginosamente a la nube. "Qué efecto tiene esto?", pregunta Gilpérez, "Pues que hay que securizar también el entorno cloud. La transformación digital nos lleva a ello igual que estar viviendo en un entorno cada vez más colaborativo, que está provocando un aumento de la cantidad de información que compartimos". El directivo concluye que "somos más colaborativos, más digitales, más adaptados al entorno cloud y estamos asistiendo a una evolución que, hasta ahora, era lineal y que, en adelante y durante los próximos cinco años, va a ser exponencial".

El usuario, el dispositivo y el dato: los tres retos clave de la ciberseguridad

Justo en el período precedente al coronavirus, las organizaciones habían planificado sus presupuestos para el 2020 con unas prioridades muy definidas. Hasta la etapa del confinamiento, "en las empresas la fuerza laboral que teletrabajaba no superaba el 10%, casi ninguna compañía estaba

preparada para que el 100% de los empleados trabajase en remoto, como finalmente ha sucedido", indica **Javier Modúbar, CEO de Ingecom.** "Con la llegada de la pandemia, los CIOs y los CISOs han tenido que cambiar sus prioridades. Hay informes que indican que hasta el 98% de los responsables de seguridad de las empresas han redefinido sus prioridades tras la pandemia, optando ahora por soluciones de seguridad asociadas al teletrabajo".

Durante el confinamiento, sin duda, la principal prioridad ha sido garantizar a los empleados una conexión en sus casas igual a la que tenían en su puesto en la oficina. Ha habido que dimensionar las conexiones VPN desde los hogares de los trabajadores.

La siguiente prioridad ha sido asegurar a toda la fuerza de trabajo en remoto. Las organizaciones contaban con una securización en sus instalaciones robusta, porque llevaban años desarrollándola, pero el entorno del hogar no tiene un sistema de seguridad informático parejo. Igualar esta securización con los dispositivos de la empresa es crucial, porque ahora el perímetro de la red se ha difuminado.

"Actualmente, la seguridad empresarial debe apoyarse en tres pilares: la persona, el dispositivo por el que se conecta dicha persona y en el dato que está manejando", apunta el CEO de Ingecom. "La persona es el elemento más vulnerable y los ciberatacantes se centran en los empleados. Curiosamente, el teletrabajador se siente seguro en casa cuando el escenario real indica todo lo contrario, esa seguridad del usuario se puede traducir como "tranquilidad" pero es contraria al concepto de ciberseguridad o de "estar en un entorno ciberseguro". El primer paso a dar por parte de las organizaciones es de concienciación, hay que educar e informar al usuario sobre las tecnologías de seguridad que utilizar, sobre los agujeros de seguridad que surgen como un malware o un ransomware. Antes las empresas veían cómo los ataques llegaban a la infraestructura IT de sus instalaciones, ahora entran en la casa del teletrabajador a través de un correo electrónico", cuenta Javier Modúbar.

"El siguiente paso que tienen que dar las organizaciones es apostar por UEBA (User and Entity Behavior Analytics) que nos permite detectar amenazas antes de que se produzcan basándonos en parámetros del comportamiento humano. Los atacantes utilizan a las personas sin que estas lo sepan para implantar elementos dañinos en la empresa. Esta es la tendencia a la que nos dirigimos cuando hablamos del elemento humano de la ciberseguridad", detalla el responsable de Ingecom.

En cuanto al dispositivo, tradicionalmente la ciberseguridad está mucho más madura, ya que buen número de empresas cuenta con tecnologías EDR avanzadas y tecnologías de detección de vulnerabilidades de parcheo capaces de atajar los ataques a dispositivos que acceden a través de un navegador y llegan hasta las aplicaciones de la compañía. "La clave aquí es controlar qué aplicaciones son más vulnerables, por ejemplo, aquellas aplicaciones legacy sin securizar, y optar por

aplicar tecnología de virtual patching en ellas para garantizar la seguridad en este ámbito", señala Modúbar.

Finalmente, con respecto al dato, el CEO de Ingecom, añade que "lo primero que hay que saber es dónde está el dato. Muchas empresas no saben donde tienen distribuidos sus datos ahora que la información ya no está en la oficina. Resulta imprescindible definir dónde está la información crítica de las organizaciones. La transformación digital está acelerando dar una respuesta a esta necesidad, tenemos que contar con una tecnología que nos asegure dónde está la información digital de la empresa".

Una vez acometido el paso anterior, hay que proteger el dato. "La seguridad no existe al cien por cien", reconoce Modúbar, "pero una vez que hemos educado al humano y securizado los dispositivos que utiliza, nos queda proteger el dato que maneja. En el último ransomware, se ha visto que los atacantes extraen los datos de las organizaciones y si éstas se niegan a pagar, les amenazan con publicar en internet su información crítica, es decir, atacan por el lado reputacional. Siempre hay que securizar las tres barreras".

Proteger el dato, objetivo de la inversión en seguridad

Hasta ahora, las organizaciones aplicaban la protección por capas, situando en la cúspide de la pirámide al dato. El principal problema es que ahora el perímetro de seguridad de las empresas ha desaparecido desde la implementación a marchas forzosas del teletrabajo. A día de hoy, los datos se encuentran distribuidos tanto dentro como fuera de la empresa o, incluso, en los propios hogares de los trabajadores, por lo que el modelo del "foso y castillo" ha dejado de funcionar.

"Las organizaciones implementan soluciones de firewall en la red o de proxy en los dispositivos, pero en el fondo lo que quieren es proteger la información más crítica. El atacante cuando se cuela en la red de una empresa busca acceder a ciertos datos sensibles ya sea de la propia organización o de sus clientes. Por ello, debemos construir un modelo de seguridad basado en la protección del dato esté donde esté", aconseja **Luis Ángel del Valle, CEO de SealPath**.

El modelo de Zero Trust, que surgió hace varios años, se ha convertido ahora en tendencia, ya que como su propio nombre indica, "debemos pasar de un modelo de confianza y vigilancia a un enfoque de confianza cero", explica el ejecutivo. Los pilares de este modelo son securizar el acceso a todos los recursos de la empresa, independientemente de dónde estén; adoptar la estrategia del menor privilegio posible; e inspeccionar y monitorizar los patrones de comportamiento de los usuarios.

En este sentido, el cifrado de la información crítica es una de las formas más efectivas para mitigar los efectos de un ataque. Sin embargo, según los datos que manejamos, tan sólo en el 2,2% de las fugas de datos se utilizó esta técnica. Esto se debe a que es una herramienta poco intuitiva, los

usuarios no tienen claro qué cifrar y qué no y, además, debe funcionar bien con otras aplicaciones corporativas.

“Cada usuario de la organización debe tener a su alcance herramientas que le permitan proteger los datos. Por eso, desde SealPath, vamos un paso más allá del cifrado. En concreto, nuestra herramienta permite proteger la información, independientemente de dónde se encuentre, así como controlar quién accede a los datos y con qué permisos”, nos recuerda Del Valle.

En concreto, SealPath permite proteger los documentos y aplicar controles de acceso dependiendo del papel de cada usuario (editar, copiar y pegar, desproteger la información y reenviarla, entre otros aspectos). Incluso, es posible eliminar un documento en remoto o quitar los permisos del documento a una persona que ya no pertenece a la empresa, evitando así la fuga de información.

“SealPath proporciona una capa extra de protección ya sea en casa, en la nube o cuando se envía a terceros. Necesitamos herramientas que sean capaces de proteger y controlar la información allí donde esté y que podamos decidir quién accede a la protección y cuándo”, concluye el directivo.

SealPath está presente en más de 20 países y trabaja a través del canal con Ingecom tanto en Iberia como en Italia. Además, se integra con tecnologías como DLP o de clasificación del dato.

Contacto de prensa:

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