Seguridad gestionada para afrontar la protección de una fuerza laboral distribuida

Áreas como la seguridad *cloud*, la gestión de credenciales, la implantación de soluciones de autenticación multifactor y el parcheo son, para Carlos Vieira, *country manager* de WatchGuard en España y Portugal, las que más se han mejorado en los últimos años.

Y es que el teletrabajo llegó con la misma fuerza que lo hizo la covid-19. Esta modalidad laboral, nueva para muchos, derribó el perímetro tradicional de seguridad de las empresas. Unas fortalezas que los equipos de TI habían levantando con muchas horas de trabajo pero que dejaron de tener sentido cuando las organizaciones se encontraron con una fuerza laboral distribuida.

Olga Romero

En cuestión de días los responsables de tecnología tuvieron que dar respuesta a numerosos retos como la descentralización de los usuarios, los cuales estaban trabajando y accediendo a los datos e información de la empresa desde múltiples puntos utilizando, algunos de ellos, sus ordenadores personales. A esto se le sumó la implementación de nuevas herramientas y la necesidad de ampliar el ancho de banda de Internet para poder utilizar estas nuevas soluciones.

Un completo cambio de paradigma que, como explica Vieira, "obligó a las empresas a apostar por soluciones de seguridad más avanzadas porque el antivirus tradicional ya no daba esa respuesta total y necesaria para garantizar la seguridad del nuevo puesto de trabajo". Por ello la instalación de herramientas de *endpoint detection and response* (EDR) se convirtió en una prioridad para pymes y autónomos. Rápidamente llegó también la preocupación por asegurarse de que quién se conectaba y accedía a las aplicaciones era quién decía ser, así como por garantizar la seguridad de las aplicaciones. Esto llevó a la implementación de soluciones de gestión de credenciales, de autenticación multifactor y parcheo.

"La seguridad del cloud, gestión de credenciales, soluciones de autenticación multifactor y el parcheo son las áreas que más han mejorado en estos años"

Y, como no podría ser de otra manera, en la era del teletrabajo la seguridad *cloud* ha sido otra de las áreas en las que más han trabajado las empresas en los dos últimos años. "A medida que empezamos a trabajar en entornos remotos los datos se trasladaron al *cloud* y había que conectar a los empleados con ese *cloud* que, a su vez, tenía que estar protegido", comenta el responsable de WatchGuard en el mercado ibérico.

Sin embargo, no solo pymes y autónomos han evolucionado sus planes de seguridad en estos dos años. Los malhechores digitales también han aprovechado este tiempo para desplegar sus armas, cada vez más sofisticadas, y colarse por las numerosas brechas de seguridad que tenían las organizaciones. Además, han variado sus objetivos. Al principio de la pandemia centraron sus esfuerzos en las grandes corporaciones, pero pronto se dieron cuenta de que "estas empresas disponían de múltiples tecnologías, metodologías y herramientas para mitigar los ataques", señala Vieira. Esto hizo que redirigiesen sus ojos hacía pymes y autónomos, "los eslabones más débiles de la cadena".

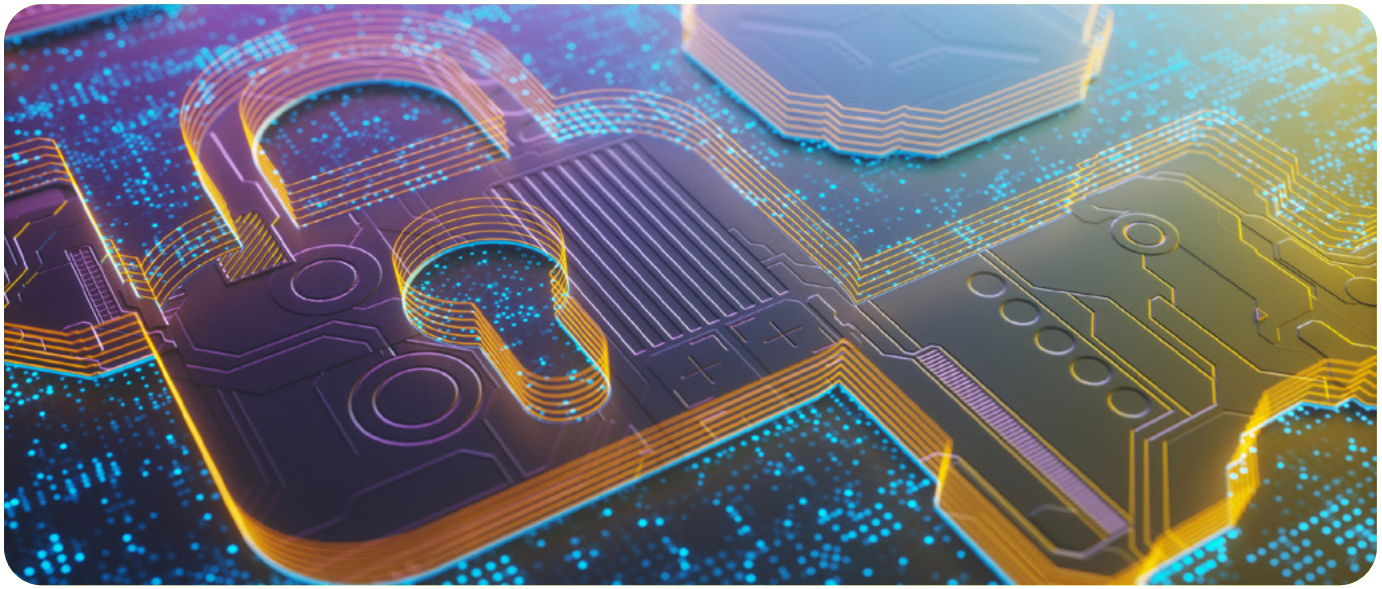
Hay que tener en cuenta también que, tal y como explica el directivo, "gracias a la automatización de los ataques a los *hackers* les resulta más rentable bloquear a una empresa de 100 empleados que carece de soluciones de *backup* y de *recover*,

ya que estas carencias las obligará a pagar antes el rescate".

En definitiva, el nuevo modelo de trabajo sumado a la automatización y sofisticación de los ataques han provocado que la seguridad se haya vuelto un área compleja de gestionar para las pequeñas empresas. Por este motivo cada vez son más las pymes que apuestan por poner esta materia en manos de profesionales. ¿Cómo lo hacen? Contratando servicios de seguridad gestionada. Una demanda en alza que, como afirma Vieira, está provocando "la transformación del modelo de negocio del canal que trabaja con las pymes, las cuales apuestan por los *partners* con *expertise* en la parte de ciberseguridad".

Concienciación y formación para frenar el *phishing*

En la nueva era digital en la que nos encontramos las habilidades digitales se han vuelto imprescindibles. Pero también lo son la concienciación y formación de los empleados en materia de ciberseguridad. Y es que, en un momento en el que los ciberataques no dejan de incrementarse, formar y concienciar a los trabajadores puede ser el mejor cortafuego para frenar algunos ataques como el *phishing*.



"Durante este periodo el *phishing* ha aumentado gradualmente y se ha convertido en un problema grave tanto para empresas pequeñas como grandes", apunta el directivo. Un problema del que, como asegura, "las empresas son conscientes y están invirtiendo cada vez más en formación y concienciación de sus trabajadores". Sin embargo, para el responsable del negocio de WatchGuard en España y Portugal, "todavía queda mucho camino por recorrer".

WatchGuard, que lleva años concienciando a sus *partners* y clientes de esta problemática, está comprometido con la concienciación y formación de los usuarios y para ello tiene en marcha una sólida estrategia de comunicación a través de los medios de comunicación, las redes sociales de la compañía y diferentes campañas

de *emailing*. Unas acciones dirigidas a alertar a los usuarios de los peligros que conlleva abrir un enlace sospechoso recibido vía correo electrónico, SMS o WhatsApp.

Además, WatchGuard dispone de dos herramientas *antiphishing* capaces de detectar y parar los ataques, a pesar de que este tipo de amenazas cada vez son más sofisticadas y emplean direcciones de correos creíbles, logos perfectos y las personas que firman son reales.

Fuerza laboral distribuida, ¿cómo garantizar su seguridad?

Poco, más bien nada, queda de ese perímetro tradicional que las organizaciones habían construido para garantizar la seguridad de sus activos. El teletrabajo ha traído consigo la descentralización de usuarios y datos o lo que es lo mismo, el mayor reto para los equipos de TI.

"Hace cinco años la arquitectura de red de seguridad de las organizaciones era realmente sencilla, el 90 % de las empresas tenían a sus empleados trabajando en la oficina con un *firewall* y todas las comunicaciones eran analizadas por el UTM", explica Vieira. Pero llegó el trabajo remoto y ese cortafuegos ya no era suficiente porque la información ya no estaba en la oficina, estaba en el *cloud*, en los ordenadores de los empleados, en sus emails.

"Cada vez más partners están ofreciendo servicios de seguridad gestionada para cubrir la amplia demanda por parte de las pymes"

Este nuevo escenario ha complicado la labor de los responsables TI que necesitan implementar más tecnologías y más avanzadas para garantizar la protección de usuarios y datos. "Creo que avanzamos hacia un enfoque de *Secure Access Service Edge* (SASE por sus siglas en inglés) en el que todos los activos estén protegidos independientemente de dónde se encuentren", afirma Vieira. Y ese, a su vez, es el gran desafío de tener una fuerza laboral distribuida. "El reto de las empresas actualmente es tener todo protegido, desde el *cloud* hasta los *endpoints* pasando por las aplicaciones", subraya. Un desafío que pymes y autónomos no pueden asumir y dejan en manos de *partners* que les ofrecen servicios de seguridad gestionada.

En este nuevo panorama "los fabricantes también jugamos un papel clave", apunta el directivo. Desde WatchGuard ofrecen su USP (*Unified Security Plarform*), una plataforma de seguridad unificada que integra soluciones para la protección de la nube, del perímetro y de los *endopoints*.

Descubre la seguridad unificada de WatchGuard para un mundo en reconexión.

"Las empresas están invirtiendo mucho en formación y concienciación de sus empleados, pero es verdad que todavía queda mucho camino por delante"

Zero trust, protegiendo el nuevo entorno laboral

El enfoque de seguridad zero trust, basado en "nunca confiar, siempre verificar", lleva existiendo más de una década. A pesar de ello es ahora cuando ha ganado un gran protagonismo debido al trabajo híbrido. Este enfoque defiende que las empresas apliquen restricciones de seguridad fuertes que les garanticen la protección de los activos, mayor visibilidad y la migración al *cloud* de una manera rápida y sencilla.

La estrategia de confianza cero de WatchGuard aborda las tres patas claves para las empresas. Por un lado, la seguridad de red que se garantiza gracias a su plataforma USP. Por otro lado, la protección de la identidad de los usuarios a través de soluciones de autenticación multifactor como WatchGuard AuthPoint. Y, por último, la seguridad de los *endpoints* con sus soluciones de EDR.

Todas estas herramientas, así como los productos y servicios incorporados en las adquisiciones que el fabricante ha hecho en los últimos tiempos, pueden gestionarse y administrarse desde WatchGuard Cloud, también conocido como "punto único de gestión".

Vieira, además, hace especial hincapié en la importancia que tiene actualmente que las empresas implementen soluciones de autenticación de múltiples factores (MFA por sus siglas en inglés). "Las herramientas MFA son la tecnología de seguridad más económica capaz de resolver millones de problemas, porque muchos ataques empiezan por el robo de credenciales", explica. Sin embargo, el directivo lamenta que todavía existan muchas empresas que no hayan descubierto este tipo de soluciones.

Oferta Kit Digital

Se espera que el nivel de digitalización del tejido empresarial español aumente gracias a los fondos NextGenerationEU. Parte de estas ayudas europeas se destinarán al programa Kit Digital, un plan puesto en marcha por el Gobierno y que se divide en 10 epígrafes de los que el IX y X están dirigidos a las comunicaciones seguras y la ciberseguridad, respectivamente.

"Los fabricantes, mayoristas y *partners* confiamos que el programa Kit Digital sirva para impulsar la transformación digital de la micro y pequeña empresa", comenta Vieira. Por este motivo las empresas tecnológicas han diseñado ofertas especiales para que las pymes, a través de los agentes digitalizadores, puedan implementar las soluciones digitales necesarias para mejorar su digitalización y, por consiguiente, su competitividad.

"Las soluciones MFA pueden frenar muchos ataques que tienen como origen el robo de credenciales"

En WatchGuard, como explica el responsable del negocio para el mercado ibérico, "hemos trabajado con nuestros mayorista y nuestro canal para, por un lado, ayudarles a acreditarse como agentes digitalizadores y, por otro lado, para que puedan ofrecer nuestra oferta a sus clientes una vez obtengan la acreditación de agente digitalizador".

Por el momento WatchGuard cuenta con cerca de 80 *partners* acreditados como agentes digitalizadores y esperan, en palabras de Vieira, alcanzar los 120 socios con esta acreditación a final de año.

Además, el fabricante ha desarrollado dos *packs*, uno para cada epígrafe, en los que se incluyen diferentes soluciones para garantizar unas comunicaciones seguras y la protección de la compañía. Para el *apartado IX, comunicaciones seguras*, el fabricante ofrece WatchGuard FireboxV y WatchGuard Basic Security. Gracias a estas herramientas las pymes obtienen servicios de SSL, cifrado de extremo a extremo, logs de conexión, control de acceso, dispositivos móviles, así como configuración inicial y actualización de seguridad.

En cuanto al *epígrafe X, ciberseguridad*, WatchGuard ha puesto a disposición de pymes y autónomos sus herramientas WatchGuard EPDR, WatchGuard Patch Management y WatchGuard Email Protection con el objetivo de proporcionales servicios como, por ejemplo, *antimalware*, *antispyware*, correo seguro, *antispam*, navegación segura o control de contenidos, entre otros.