Seguridad Digital, la gran oportunidad para el canal TI en 2019

Seguridad avanzada para nuevas amenazas

Las ciberamenazas crecen en cantidad y sofisticación, por eso se hace cada vez más necesaria una aproximación a la seguridad más proactiva que reactiva, que tenga en cuenta el número y variedad de los dispositivos conectados a la red empresarial, los permisos de acceso de los usuarios, políticas que acompañen al dato en su recorrido por la infraestructuras híbrida. Una seguridad que ofrezca una respuesta efectiva a la amenaza, y que además cumpla con las diferentes normativas y sea fácil de gestionar. **Rosalía Arroyo.** Formigal

Aqué se enfrentan las empresas o cómo ayudarlas a hacer frente a los retos son algunas de las cuestiones que se plantearon durante un encuentro que reunió a los fabricantes líderes del sector para debatir el estado de la seguridad y su futuro más próximo.

Con Formigal como fondo la mesa redonda contó con la participación de Conrado Crespo, Senior Sales Engineer de CounterCraft; Alejandro Campos, Channel Account Manager de Check Point; Juan Asensio Múñoz, Country Manager Spain & Portugal de A10 Networks; Félix Martos, Security Channel Manager Spain & Portugal de Aruba; Carlos Muñoz, Senior Presales Engineer Security Advisor de McAfee, y Alberto López, Director Enterprise Security de V-Valley.

Moderada por Rosalía Arroyo, directora de IT Digital Security, la mesa redonda arrancó planteando qué es lo que se está viendo en el mercado desde el punto de vista de seguridad. Según Conrado Crespo, aunque se mantiene la atención en soluciones de ciberseguridad que tienden a contener, se está intentando dar un salto de paradigma "porque no todo es contención". Menciona el ejecutivo de CounterCraft las teorías de honeypots y la detección de amenazas llevando a los ata-

cantes a entornos sintéticos, que es a lo que se dedica CounterCraft, una empresa con tres años de vida, unos 30 empleados, con clientes en entornos de alta criticidad y que busca "partners de valor añadido".

Menciona Alejandro Campos que las empresas evolucionan y que, aunque hace tiempo que se habla de ello, es ahora cuando están empezando a acometer, o ya tienen, proyectos de migración al cloud o proyectos de movilidad, entornos que han hecho saltar los perímetros de seguridad. "Hoy en día la protección perimetral es insuficiente para proteger los nuevos vectores de ataque y nosotros como fabricantes tenemos que ampliar nuestro alcance a todas las alternativas", asegura el ejecutivo.

Sobre la problemática a la que se enfrentan las empresas, dice Juan Asensio que "es la de siempre: cómo ser más ágiles para proveer un mejor servicio a sus clientes o cómo dar un producto en el menor tiempo posible". Menciona el papel fundamental del cloud para hacer frente a la problemática y menciona también el reto del tráfico cifrado, que siendo más del 60% del tráfico mundial pone en serias dificultades a algunos equipos, ciegos a lo que está saliendo de la organización. Llegados a este punto, los fabricantes se tienen que adaptar a un entorno híbrido y al mismo tiempo proporcionar visibilidad de lo que está pasando en la red.

Félix Martos incide en la pérdida de perímetro, añade que los ataques están cada vez más dirigidos y financiados, que la superficie de ataque ha aumentado y finalmente que las plantillas de especialistas se van reduciendo. Todo esto, "que es un problema para las empresas y una oportunidad para nosotros, nos lleva a los servicios gestionados", los únicos capaces de hacer frente a toda la problemática.

Carlos Muñoz recuerda la entrada en vigor, el año pasado, de la nueva regulación de protección de datos, algo "que ha marcado cómo las organizaciones han ido consumiendo servicios de seguridad y qué necesidades intentaban cubrir"; a GDPR, y al movimiento hacia los entornos cloud, le siguió un gran interés por el Shadow IT y, como consecuencia de ello, una gran demanda de soluciones tipo CASB para la protección de entornos SaaS. Pero la maquinaria estaba en marcha y a finales de 2018 ya se empezaba a ver un siguiente paso hacia el modelo cloud: la migración de cargas de trabajo a infraestructuras como servicio. "Vemos que todo cambia",

"Hay que **facilitar el trabajo de los partners** con consolas y propuestas que les permitan **dar el valor que se les supone que deben dar**"

Conrado Crespo,
Senior Sales Engineer,
CounterCraft

SEGURIDAD DIGITAL, LA GRAN OPORTUNIDAD PARA EL CANAL TI EN 2019

dice el directivo de McAfee, "vemos cómo las empresas empiezan a preguntarse qué hago con mis cargas de trabajo una vez las tengo implementadas en un entorno como AWS", y ya no se habla de infraestructura como servicio, sino de plataforma como servicio.

El nuevo paradigma es un entorno híbrido, con tráfico norte-sur y también este-oeste, en el que las compañías "quieren saber si las prácticas de seguridad que están aplicando sobre ese data center cloud están reguladas y se pueden considerar buenas prácticas". Se añade una evolución de los puestos de trabajo "que se han convertido en un elemento muy interesante para todas las organizaciones. Las soluciones EDR se basan en elementos de protección que de algún modo se basan en información originada en el puesto de trabajo".

Ante toda esta problemática lo que propone V-Valley son soluciones, y cómo puede hacerse un cross selling, "cómo A10 abre el tráfico cifrado y lo manda al IPS de McAfee, por ejemplo" dice Alberto López, añadiendo que el objetivo es "construir un porfolio, establecer un soporte tanto preventa como postventa avanzados, y ayudaros en los proyectos y poner valor".

> Estamos haciendo que la **seguridad** sea una **oportunidad de negocio**. Y el dinero no viene de revender soluciones, sino de integrarlas y ser capaces de **proporcionarle al cliente una solución integrada** que aporte valor
>
> Félix Martos, Security Channel Manager Spain & Portugal, **Aruba**

VISIBILIDAD Y ENDPOINT, DOS VARIABLES IMPRESCINDIBLES

Los comentarios de los ponentes dejan claro que la visibilidad es un elemento fundamental dentro de una estrategia de seguridad, y que el endpoint, relegado dentro del perímetro que establecieron los firewalls hace una década, recobra un papel protagonista con la movilidad y el cloud.

Dice Conrado Crespo, Senior Sales Engineer de CounterCraft, que con herramientas como los EDR quizá tengamos ahora demasiada visibilidad porque la información hay que procesarla "y el coste de los equipos de SOC a la hora de separar el grano de la paja tiene un coste muy elevado". Llegados a este punto las tecnologías del engaño, o de cyberdeception "empiezan a tener cierto sentido en coordinación con otras tecnologías de defensa del endpoint o de defensa perimétrica, en cuanto que tú depositas unas trampas y salta es una alerta confirmada". Estos datos, ya confirmados, junto con los aportados por los SIEM y la ruta de ataque genera información e inteligencia para luchar contra las amenazas.

"Las empresas son cada vez más conscientes de que el endpoint es cada vez más importante", dice Alejandro Campos, Channel Account Manager de Check Point. Y es que en el momento en que

irrumpen los portátiles, las tablets, los smartphones, se multiplican los vectores de ataque, algo que se complica cuando se tiene en cuenta que es estos dispositivos cada vez se utilizan más para trabajar. Es ahora cuando las empresas se están dando cuenta de la problemática.

Para Juan Asensio, Country Manager de A10 Networks, se está produciendo una clara disrupción del tema de la visibilidad. No sólo el escándalo de la NSA desató las preocupaciones, es que Google promueve el tráfico cifrado, que no deja de crecer, y eso hace que se esté perdiendo el rastro de los que está pasando por la red. "En A10 estamos viendo un montón de proyectos relacionados con esto y nos alegra porque estamos proporcionando una solución que ayuda a los firewalls, a los IPS, a los antivirus… a seguir haciendo su trabajo".

La visibilidad es para Aruba uno de los cuatro pilares de la seguridad. Explica Félix Martos, Security Channel Manager Spain & Portugal de Aruba, que en la mayoría de los casos los responsables de seguridad de las empresas no saben qué dispositivos hay en la red, y que es ahora cuando empiezan a darse cuenta de la necesidad de tomar el control". Asegura el directivo que para la seguridad la visibilidad es la mitad del trabajo, y el siguiente paso es la protección. "Estamos haciendo que la seguridad sea una oportunidad de negocio. Y el dinero no viene de revender soluciones, sino de integrarlas y ser capaces de proporcionarle al cliente una solución integrada que aporte valor", reflexiona Martos.

Para Carlos Muñoz, Senior Presales Engineer Security Advisor de McAfee, "es necesario contar con una infraestructura capaz de entender la visibilidad de una manera holística", y habla de que la respuesta a una amenaza no sólo tiene que basarse en que las soluciones puedan hablar entre ellas por medio de una API, sino "de utilizar metodologías comunes". Menciona McAfee DXL (Data Exchange Layer), un protocolo desarrollado por su compañía, open source desde 2016 y que cuenta con unas 140 integraciones con diferentes fabricantes de seguridad "para hacer que lo que detecte uno se convierta en visibilidad en la reacción del resto".

PLATAFORMAS Y SERVICIOS GESTIONADOS

Recurrir a un proveedor de servicios de seguridad gestionada es una opción que siempre está encima de la mesa. Estos servicios pueden ser la solución para disponer de personal experto y hacer frente a las amenazas. Entre las grandes ventajas

"Estamos pasando de comprar equipos o licencias a **comprar servicios integrados** por diferentes fabricantes capaces de integrarse"

Alberto López, Director Enterprise Security, **V-Valley**

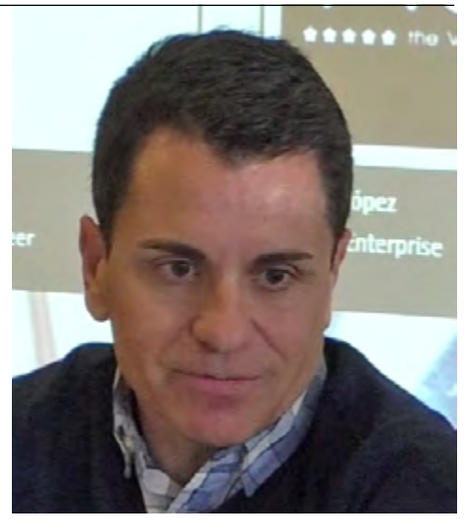
mencionar que, al externalizar los servicios de ciberseguridad, una compañía consigue experiencia y calidad de servicio, así como una posible reducción de costes

Es una manera de que las empresas, los clientes, se dediquen a sus negocios, dice Alberto López, de V-Valley. Con el tiempo, las amenazas son más y más sofisticadas y eso ha obligado a muchas empresas a ir añadiendo elementos de seguridad que hacen que cada vez sea más complicado mantener la seguridad de manera óptima, y por tanto a buscar quién les gestione la seguridad. "Está ocurriendo, estamos pasando de comprar equipos o licencias a comprar servicios integrados por diferentes fabricantes capaces de integrarse", asegura el directivo de V-Valley.

Sobre las ventajas que las plataformas y los servicios ofrecen a los clientes, dice Carlos Muñoz que las primeras socializan los servicios "que de otra manera no podrían llegar a las empresas" y los segundos resuelven el problema del talento necesario para hacer frente a la seguridad. Añade el directivo de McAfee que dentro de tres años no se tratará de proteger el servidor o el terminal porque ya no pertenecerán a la empresa, sino de los accesos "en un modelo donde la información está sustentada sobre plataformas que funcionan mediante pago por uso", para lo que será de vital importancia el análisis de comportamiento. "Creo firmemente en que vamos a estar ahí, que incluso los integradores tienen que encontrar la manera de añadir valor a esas plataforma de AWS, de Azure… y creo que es la única manera por parte de las organizaciones de tener una seguridad competitiva", añade.

"Los servicios gestionados están permitiendo que las empresas se dediquen a sus cosas y no tengan que tener equipos especializados que seguramente vayan a utilizar en muy pocos momentos de su vida", die Félix Martos. Añade el directivo de Aruba que un proveedor de servicios de seguridad gestionada puede aportar el talento y compartir el coste entre todos sus clientes para que éstos puedan tener acceso a seguridad de primera nivel, y coincide en que el análisis de comportamiento es fundamental porque en la mayoría de los casos las amenazas no son conocidas; "ni siquiera sabemos cuál va a ser la próxima amenazas y el que no tenga un UEBA va a tener serios problemas", avisa.

> "Las fronteras ya no están tan claras y estamos en un **momento clave de cambio**, y los **proveedores tendremos que reinventarnos** y ver dónde está el negocio"
>
> Juan Asensio Múñoz, Country Manager Spain & Portugal, **A10 Networks**



Asegura Juan Asensio que hay que reinventarse porque "el paradigma de tengo una caja y estoy gestionándola deja de existir; el paradigma de tengo que ir a trabajar a un sitio está empezando a dejar de existir. Las fronteras ya no están tan claras y estamos en un momento clave de cambio, y los proveedores tendremos que reinventarnos y ver dónde está el negocio".

Los servicios de seguridad gestionada son imprescindibles porque si hace años

se tenían que proteger entornos muy controlados, ahora la situación ha cambiado, dice Alejandro Campos, de Check Point. Han aparecido muchos vectores de ataque y una empresa no se puede permitir tener expertos en seguridad para cada uno de esos entornos; "la solución está en el canal, en empresas especializadas, y por eso triunfan los servicios gestionados. Para poder securizar todo tu entono tienes que delegar esa tarea en otras empresas", añade.

Hay que ponerse los zapatos de los integradores, aseguraba Conrado Crespo, planteando cómo los fabricantes tienen que responder a demandas relacionadas con ofertas multitenancy, capaces de aislar diferentes entornos y áreas administrativas para diferentes clientes, o los servicios que el canal puede ofrecer sobre la tecnología. Aseguraba el directivo de CounterCraft que hay que facilitar el trabajo de los partners con consolas y propuestas que "les permitan dar el valor que se les supone que deben dar".

EL CANAL HABLA

Tras el debate de fabricantes, donde queda claro que aún queda mucho negocio que ofrecer, mucho que alumbrar en el mundo de la seguridad, muchos vectores que proteger y también mucho por descubrir, se pasa el testigo a los partners. ¿Se sienten arropados por los fabricantes? En un mundo ideal ¿qué pedirían? ¿qué temen?

Se asegura que al canal le gusta colaborar con los fabricantes y que estén presentes. También se menciona la competencia entre integradores y cómo a veces es difícil salvar el margen; añadir valor es la diferencia.

Se plantea que no hay tantos proveedores de cloud, apenan un puñado y que esos dos, o tres, o cuatro "utilizan la tecnología que utilizan, y en muchos casos proveerán de tecnología propia"; llegados a este punto y en el medio plazo, "¿qué va a ser de todos nosotros?".

Contestan los fabricantes asegurando que hay empresas que trabajan al mismo tiempo con varios proveedores de cloud y que uno de los problemas que se le plantean es cómo puede definirse una política de seguridad que se aplique tanto en los entornos on-premise como en las máquinas que voy a tener en mi datacenter híbrido, en las del proveedor pequeñito que está ofreciendo un servicio concreto y además tiene su infraestructuras virtualizada en AWS, en Azure o en Google… Y la política tienen que ser una, y eso es un servicio que se demanda y que está en manos del canal.

Si hablamos de CASB, es el integrador el único que pueden sacar provecho de una

"Los servicios **de seguridad gestionada son imprescindibles** porque si hace años se tenían que proteger entornos muy controlados, ahora la situación ha cambiado"

Alejandro Campos, Channel Account Manager, **Check Point**

solución de este tipo. Lo que debería preguntarse ese integrador es si el fabricante ha trabajado para hacer que su solución de CASB sea multitenant y tenga una vista desde la perspectiva del integrador para que cuando se conecte vea a los 40 o 30 clientes a los que está prestando servicio, pueda aplicar una policía de seguridad unificada para todos ellos, o pueda definir un servicio proactivo de notificaciones; esto es lo que marca la diferencia de un proveedor de servicios a otro.

La conclusión por parte de los fabricantes es que los proveedores de servicios cloud no sólo no van a impedir las ventas, sino que van a abrir una oportunidad muy grande de poder comercializar otro tipo de soluciones.

La falta de talento de la que tanto se habla, ¿también afecta al canal? Sí, para el tema del cloud hace falta mucho conocimiento. Y hablando del nube, se va, pero a qué ritmo, con qué tipologías y quién se va a hacer cargo de proteger la nube; son preguntas que se plantean y se contestan hablando de entregar al cliente una solución unificada. En todo caso, está claro que no se trata sólo de si hay talento o no, sino que el paradigma también está en hacia dónde se va y cuánto tiempo se va a tardar, incluso de si ahora tiene sentido un cambio en el tipo de licenciamiento porque aún hay mucha planta on premise.

Se plantean los licenciamientos dinámicos, que ya existen, y en los que se paga por número de eventos de seguridad o por gigas. Parece claro que hay opciones y un largo camino por recorrer. Las oportunidades están ahí y el valor añadido lo pones tú. ■

> **Las plataformas socializan servicios** que de otra manera no podrían llegar a las empresas y los **servicios gestionados resuelven el problema del talento** necesario para hacer frente a la seguridad
>
> Carlos Muñoz, Senior Presales Engineer Security Advisor, **McAfee**