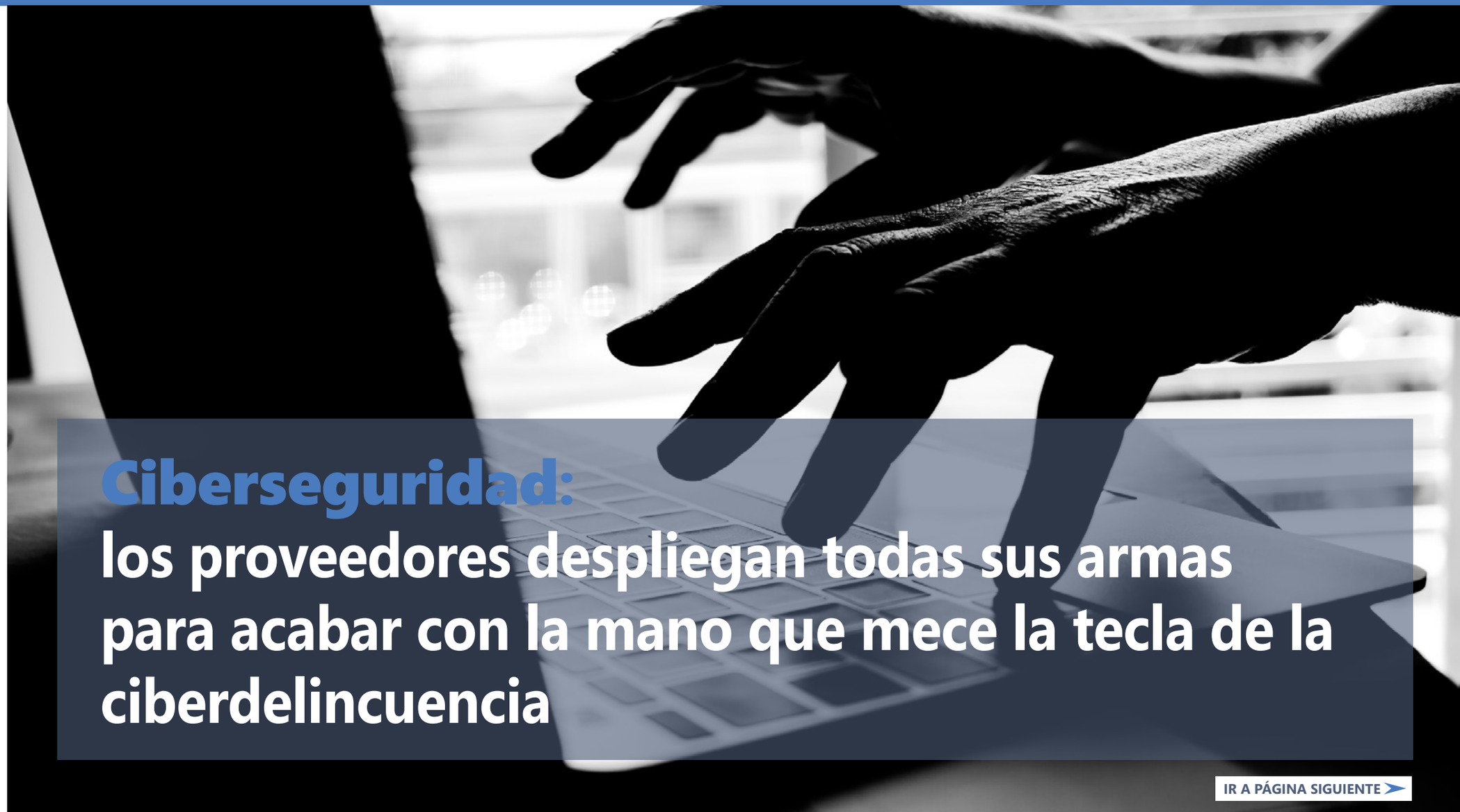
GUÍA 2023 Ciberseguridad

directorTIC Información de valor para la toma de decisiones

ESPECIAL DIRECTOR TIC 2023



Ciberseguridad:

los proveedores despliegan todas sus armas para acabar con la mano que mece la tecla de la ciberdelincuencia

IR A PÁGINA SIGUIENTE

Los ciberdelincuentes no dan un respiro

Cada once segundos una empresa sufre un ataque de *ransomware*. Así lo pone de manifiesto ENISA, mientras Innovery destaca el crecimiento de ciberataques que están recibiendo sectores como el de educación, sanitario, administraciones públicas o *e-commerce*. Este último, el más perjudicado, con un 49 % más de ataques en lo que va de año, aunque la suma de ataques en estos sectores se ha incrementado un 8 %, con una media de 1.250 ciberataques por semana.

El *ransomware* sigue siendo el que más crece, ganando popularidad por su bajo coste, su efectividad, el impacto que causa tanto a nivel económico como reputacional y por las facilidades que existen para llevarlo a cabo. Las plataformas de *ransomware* como servicio, mediante una suscripción mensual, ayudan a los ciberdelincuentes a extender el ataque, por lo que obtienen aproximadamente un 20 % de las ganancias tras el mismo. Por ello desde Innovery consideran que esta va a seguir siendo la principal amenaza para lo que queda de 2023, aunque también advierten sobre un repunte de vulnerabilidades de *zero day* con objetivos como pequeñas empresas, *e-commerce,* Administración Pública y banca. Y recuerdan que mientras siga activo el conflicto entre Ucrania y Rusia, la ciberguerra continuará afectando a los países en función de su posicionamiento.

EDITORIAL

Confianza digital

La confianza digital también es mejorable según los datos aportados por un estudio de ISACA, llevado a cabo ante más de 8.100 profesionales de ciberseguridad a nivel mundial. Según el mismo, aunque el 82 % de las empresas europeas, el 84 % a nivel global, considera que la confianza digital es muy importante para sus organizaciones, sólo el 64 % de las empresas la prioriza a nivel mundial, el 57 % en Europa. Y sólo el 10 % de los profesionales de ciberseguridad cree completamente en la estrategia digital de sus compañías.

Teniendo en cuenta que descuidar la confianza digital implica consecuencias como el impacto negativo en la reputación, en un mayor número de incidentes de seguridad y vulnerabilidades o en una pérdida de clientes, ¿cómo debe garantizase ésta? Adoptando medidas que permitan garantizar la seguridad de la información, objeto de tratamiento en la organización y una adecuada gestión de los riesgos a los que se encuentra expuesta, inciden desde ISACA. Y "a medida que la transformación digital de una empresa o institución se consolida, es imprescindible aumentar la concienciación y la formación de los empleados en materia de seguridad", apuntan. Aunque el estudio refleja que sólo el 32 % de los profesionales afirma que su compañía ofrece formación a sus empleados para garantizar la confianza digital y un 31 % comprende cómo afecta a su organización. Más pesimista es el dato de que sólo un 13 % tiene un puesto dedicado a la confianza digital y otro 19 % reconoce que la junta directiva de su organización ha priorizado esta materia.

Una confianza digital que va a adquirir una gran relevancia con normativas como la Directiva de resiliencia en entidades críticas (cuyo objetivo es aumentar la resiliencia de las entidades críticas y su capacidad para prestar sus servicios esenciales); el Reglamento DORA (*Digital Operational Resilience Act*), sobre resiliencia operativa digital del sector financiero; y NIS2 (marco regulador general de la ciberseguridad para garantizar un elevado nivel común de seguridad en las redes y la información).

SUMARIO

Directora: Marilés de Pedro
mariles@taieditorial.es
Redactora jefe: Inma Elizalde
inma@taieditorial.es
Redactora: Rosa Martín
rmartin@taieditorial.es
Redactora: Olga Romero
olga@taieditorial.es
Publicidad: David Rico
david@taieditorial.es
Publicidad: Nuria Díaz
nuria@taieditorial.es
Producción: Marta Arias
marta@taieditorial.es

Depósito legal: M-38033-2015
ISSN: 2341-1511

Edita:
T.A.I. Editorial, S.A.
(Técnicos Asesores Informáticos Editorial, S.A.)
www.taieditorial.es
Avda. Fuencarral, 68
28108 Alcobendas (Madrid)
Tel. 91 661 61 02 - Fax: 91 661 29 28
e-mail: correo@taieditorial.es

"No sé cuál será nuestro futuro pero tenemos herramientas para prepararnos"

Según el reporte global de ciberataques del primer trimestre de 2023 de Check Point Research, división de Inteligencia de Amenazas de Check Point Software, los ataques semanales han aumentado un 7 % con respecto al mismo periodo del año anterior. Mario García, director general de Check Point Software en España y Portugal, destaca el avance que están dando los ciberdelincuentes en múltiples direcciones, de forma masiva.

El *ransomware* de doble extorsión en el que amenazan con no devolver los datos y publicarlos sigue creciendo, reconoce. Pero ahora, adicionalmente, destruyen los datos incluso sin pedir un rescate, simplemente por hacer daño, revela. "Muchas de esas armas son de origen gubernamental, pero cuando se utilizan en Internet quedan a disposición del público. Empiezan entre Estados y acaban entre empresas", advierte.

Otra tendencia que desde Check Point Software han detectado son los grupos perfectamente organizados, con objetivos claros que se coordinan entre sí a la hora de atacar, compartir datos y técnicas.

Una tercera tendencia pasa por los ataques por correo electrónico. "El 86 % llega por esta vía", asegura, "combinándolo entre empresas y personas porque para atacar a las primeras fijan su objetivo en sus empleados. Una vez conseguido el fin no explotan el ataque directamente. Lo venden a quien realmente quiere dañar a esa organización", asegura. "Esto es un mercado en el que todo se vende: las vulnerabilida-

Mario García, director general de **Check Point Software** en España y Portugal

CHECK POINT SOFTWARE

des, el *malware*...", apunta, por lo que, en su opinión, es mucho más complicado detener a los autores, aunque considera que la policía española está muy preparada en el ámbito de la ciberseguridad.

El valor de la IA

El papel de la inteligencia artificial en el ámbito de la lucha contra la ciberdelincuencia es fundamental, si bien, como constata Mario Garcia, "cuanto más listas son las herramientas, lo son en las dos direcciones: en la de defensa y en la de ataque". Check Point Software cuenta con herramientas de *deep learning*, con un conocimiento más profundo sobre cómo funcionan los ataques y 15 motores de IA junto a un motor (CADET) que toma la última decisión sobre el resto. "Utilizamos herramientas de inteligencia artificial para detectar cuándo te están atacando y ver si lo que está sucediendo es realmente un ataque", confirma. "Nuestro motor de inteligencia pregunta órdenes de magnitud por encima de lo que recibe Google en términos de información", sostiene, con la ventaja de contar con una gran cantidad de información sobre acciones maliciosas. Una base de datos sobre este tipo de actuaciones con la que construyen, usando la IA, defensas para prevenir frente a las amenazas. "Contamos con más información que los ciberdelincuentes, sobre todo el histórico de lo que ha sucedido, para lanzar herramientas más inteligentes que ellos", se reafirma. ¿Cuál será nuestro futuro? "No lo sé", responde, "pero tenemos herramientas para prepararnos".

La necesidad de mejora de las pymes

Si vamos desgranando por segmentos empresariales, las pymes están invirtiendo en SaaS, en la nube, en movilidad, pero ¿qué ocurre con la ciberseguridad? Tienen una cuenta pendiente con ella, observa Mario García, aunque "poco a poco van empezando a reaccionar".

"Una aplicación en SaaS es una buena idea pero no implica estar seguro. Tiene que hacerla segura la empresa, poner sus herramientas de

CHECK POINT SOFTWARE

seguridad, proteger sus puestos de trabajo, ordenadores, móviles, red... para que el acceso a las aplicaciones que están fuera se haga de una manera segura, y más cuando se ha puesto de moda la cadena de valor", añade. "¿Para qué quiero atacarte si puedo atacar a tu abogado, por ejemplo, y llevarme todos tus contratos? La cadena de valor es el eslabón más débil", advierte. Al tiempo que aconseja a las compañías, al contratar un servicio, preguntar con qué sistemas de protección cuentan, por si pueden ser ellos los que infecten.

¿Cómo pueden defenderse con Check Point Software? "Contamos con una gama de productos para la pyme: una solución completa a la que denominamos Infinity", confirma, una potente plataforma de gestión de seguridad con la que las organizaciones protegen y administran toda su infraestructura de TI: redes, nube, IoT, *endpoints* y dispositivos móviles. "Tenemos también una serie de iniciativas que llevamos a cabo con nuestros distribuidores para captar integradores que puedan disponer de nuestras soluciones para llegar a las pymes con nuestra mejor solución".

¿Cómo eliminar los puntos ciegos?

Desde Check Point Software recomiendan a los responsables de ciberseguridad desarrollar e implementar una estrategia de seguridad que elimine los puntos ciegos y las debilidades en todo el panorama digital. ¿Cómo? Dejándose aconsejar por profesionales, analizando cómo defenderte (con herramientas de prevención), herramienta que en el caso de Check Point Software se denomina Quantum y protege todo lo relacionado con la red, "hasta el punto de que si alguien consigue entrar en la misma no puede salir", avanza.

Otra de sus apuestas es Harmony, solución de seguridad unificada para usuarios, dispositivos y accesos que protege de los ataques más sofisticados, al tiempo que garantiza el acceso Zero Trust a las aplicaciones corporativas.

En cuanto a la nube cuentan con CloudGuard para proteger las cargas de trabajo.

Problemas en la nube

En el apartado de la nube destaca problemas como el desconocimiento en seguridad: "Pensar que por ir al *cloud* estás seguro, pero no lo estás. Quien está seguro es el proveedor, no tu información". Sin olvidar la mala configuración, para lo que existen herramientas que ayudan en este sentido. Sin embargo la adopción de las mismas es muy baja, incluso por parte de los CIO y CISO. ¿La razón? "Los CISO no están involucrados en todos los proyectos porque no es su ámbito. El CIO en muchos casos no reporta al CIO. Para el CIO lo importante es que todo funcione, no que funcione de forma segura". "Las empresas más grandes funcionan mejor", admite pero "cuanto más pequeña es la compañía, peor funciona y la nube es la gran desconocida".

En cuanto a su relación con CIO y CISO reconoce que es complicada. En función de lo que quieren hacer, Check Point Software les ayuda a hacerlo bien.

CHECK POINT SOFTWARE

Check Point Horizon: conocimiento para integradores y empresas

Check Point Software lanzó hace unos meses Check Point Horizon, una oferta "que aglutina conocimiento" porque, tal y como Mario García, director general de Check Point Software en España y Portugal, señala en este vídeo: "Contamos con mucha tecnología pero faltan personas capaces de sacar partido a la misma, profesionales que puedan gestionar las nuevas amenazas". Check Point Horizon es una plataforma de operaciones de seguridad que permite a integradores y clientes ofrecer una respuesta mucho más completa en ciberseguridad para que, en caso de ataque, las organizaciones sepan qué está ocurriendo y cómo pueden reaccionar.

¿Cómo protegerse de los ciberataques con Check Point Software?

Sanidad, educación, servicios financieros y cadena de suministro son los sectores más afectados por los ciberataques. ¿Cómo protegerse frente a las amenazas? Mario García, director general de Check Point Software en España y Portugal, avanza en este vídeo que desde la multinacional de ciberseguridad israelí ayudan a sus clientes evaluando el sector en el que se encuentran y cómo abordan los problemas a los que se enfrentan. En una segunda fase determinan qué tipo de tecnología aplicar para mejorar su nivel de seguridad y aprender a gestionar su riesgo.

FLEXXIBLE

Flexxible aborda la seguridad de las empresas con FlexxClient y FlexxDesktop

La seguridad por diseño es una de las características de Flexxible. Seguridad que también aborda en dos de sus grandes familias de productos: FlexxClient y FlexxDesktop, que aportan tanto niveles de acción como de automatización. FlexxClient mantiene, además, una alianza nativa con CrowdStrike, embebiendo un elemento de seguridad si el cliente así lo desea.

Manuel de Dios, *sales specialist director* de **Flexxible**

La tecnología con marca española se ha vuelto "profeta en su tierra". Flexxible es un ejemplo de ello. Un éxito que mantiene a nivel nacional e internacional con su plataforma que combina y simplifica la provisión de recursos y herramientas del puesto de trabajo, independientemente de dónde se consuman, ofreciendo una experiencia de usuario óptima. Para dar esta experiencia de usuario la observabilidad y visibilidad son fundamentales.

En el ámbito de la observabilidad ofrecemos "básicamente datos", reconoce Manuel de Dios, *sales specialist director* de la compañía, en un momento en el que la seguridad por diseño se ha convertido en una máxima para Flexxible. Una óptica, la de la seguridad que en muchas ocasiones ponen sus clientes, reconoce, probando esa herramienta adaptable a las necesidades de cada uno de ellos. ¿Cómo? "Recabando los datos desde nuestra plataforma FlexxClient que mide el funcionamiento, la ralentización y la actividad técnica de los dispositivos", responde. "Nuestros usuarios buscan en el conjunto general de datos factores específicos que afecten de manera crítica a un determinado tipo de aplicaciones y de disposi-

FLEXXIBLE

tivos, por lo que pueden hacer una seguridad preventiva y tener un sistema de alertas adaptado a su propia explotación de la plataforma". En su opinión, el mayor reto de la observabilidad estriba en cómo orientar la misma. "Tenemos un reto como industria. Desde Flexxible intentamos ayudar a perfilar cuáles son los objetivos y cómo vamos a leerla porque este es un concepto que aplica a todo y los clientes entienden que puede ser un elemento necesario a la hora de tomar decisiones. Nosotros hablamos de observabilidad dentro de lo que es la plataforma de dispositivos de la compañía, que es casi el 80 % de lo que vigila la misma", especifica.

FlexxClient se presenta por módulos integrados e inseparables. Tiene una visión específica para soporte, gestión y control, así como para la monitorización de la experiencia del usuario y automatización con FlexxAutomation, donde se gestionan los casos de soporte de manera automática como el cambio de claves para el usuario final, por poner algunos ejemplos.

Acceso seguro a través de escritorios virtuales

Flexxible proporciona acceso seguro desde cualquier lugar a través de sus escritorios virtuales, simplificando la seguridad de los mismos.

"La posibilidad de tener escritorios virtuales garantiza un mayor control", comenta. "Esto no es porque lo provea la capacidad de FlexxDesktop, la solución de Flexxible que maneja este aspecto, sino los *brokers* que permiten la publicación de aplicaciones y escritorios que están dentro de un centro de datos. Lo que estamos llevando es esos recursos a otro dispositivo. Aislar el uso del dispositivo siempre ha sido un elemento de prevención porque así tenemos el escritorio controlado", declara. FlexxDesktop unifica todas las tecnologías, haciendo que la gestión sea más sencilla. "Como gestor me da igual la tecnología que haya por debajo de la plataforma o dónde esté alojada porque estoy administrando ese conjunto de escritores virtuales y como usuario es totalmente transparente".

¿Qué ventajas ofrecen en cuanto a seguridad en el DaaS? "No deja huecos libres", responde. "Al tenerlo todo unificado aplico mis políticas de seguridad en la plataforma de VDI o de aplicaciones virtualizadas. No permite problemas de disfunción",

En el ámbito de la pyme cuentan entre sus clientes con organismos pequeños como los ayuntamientos en los que uno de sus problemas pasa por la escasez de recursos. "Tienen 20 o 25 sedes diferentes que dan servicios subcontratados y forman parte de la organización. Organismos en los que el mantenimiento de sus plataforma de PC en muchos casos no está virtualizada y les supone un problema. Una herramienta como FlexxClient, con un coste muy asequible, con la que pueden intervenir de manera remota, sin problemas de vulneraciones de seguridad... simplifica y ahorra muchos costes".

EDITORIAL
SUMARIO
CHECK POINT SOFTWARE
FLEXXIBLE
SONICWALL
ZYXEL

FLEXXIBLE

También cuenta con FlexxMonitoring, una *app* específica donde convergen todos los datos que se recogen para su análisis y en la que se define el vector de aproximación a la información que se desea.

CISO y CIO

"Una tecnología con la que el CISO va a contar con una información muy accesible y rápida. Una herramienta integrada en la propia explotación del negocio de la organización con la que el CISO puede medir qué está ocurriendo, con la ventaja de que no tienen que invertir en otras herramientas ya que éstas están siendo aplicadas para otras funciones, integradas dentro de su propio sistema IT", explica.

Manuel de Dios confiesa que se sienten muy reconocidos por CIO y CISO. "El acento en el entorno de la seguridad lo han ido poniendo en mayor medida nuestros clientes", incide. "En nuestra compañía no tenemos expertos en seguridad dentro del capítulo de desarrollo. Estábamos anotados en la experiencia, en

el soporte y en el diseño de la tecnología. Han sido nuestros clientes, entre los que también se encuentran los CIO, quienes han puesto mucho foco en aspectos de negocio, en huella de carbono, consumo o recursos humanos porque tienen presiones en esos medidores. Los CISO, cuando conocieron que estábamos hablando con responsables de sistemas o con responsables de *Workplace*, reconocieron que querían estar presentes en esas reuniones porque esto les afecta directamente y les interesa en gran medida".

A tener en cuenta

- **FlexxDesktop es una solución de escritorio como servicio (DaaS) donde convergen la computación en el *edge* y la computación en la nube, permitiendo que los escritorios virtuales se ejecuten en cualquier lugar.**
- **FlexxDesktop, bajo un modelo de precios de suscripción, simplifica la administración diaria y mejora la experiencia digital, con la experiencia del usuario en el centro.**
- **FlexxClient permite a las organizaciones identificar los problemas y solucionarlos de forma automatizada, gracias a la monitorización en tiempo real.**
- **FlexxClient es sinónimo de ahorro y escalabilidad, de seguridad y privacidad ya que reduce en un 30 % los *tickets* de soporte y proporciona una visión 360º de los ordenadores para priorizar los requisitos del hardware del equipo de trabajo.**

"El producto de Flexxible está pensado como un elemento seguro"

La importancia de la seguridad por diseño en los escritorios virtuales es fundamental. En Flexxible la seguridad está por diseño a todos los niveles de producto. Así lo manifiesta Manuel de Dios, *sales specialist director* de la compañía. "Toda la tecnología que subyace en términos de seguridad está integrada dentro de nuestros propios sistemas", señala en este vídeo. En el caso de FlexxClient, cuando salen del ámbito virtual, además, está montado sobre un sistema de IoT.

Flexxible: ¿cómo resolver los desafíos en torno al dato?

¿Cuáles son los grandes desafíos en torno al dato en la era del trabajo híbrido para el CIO y el CISO de las medianas-grandes corporaciones y cómo Flexxible ayuda a minimizarlos?

Manuel de Dios, *sales specialist director* de Flexxible, considera que hay que convertir el dato en un dato manejable, en conocimiento e inteligencia con el que poder tomar decisiones. Algo que consiguen en Flexxible.

Si no somos capaces de detectar, ¿cómo vamos a defender?

Según el Informe de Ciberamenazas 2023, elaborado por SonicWall, los ciberataques son cada vez más sofisticados en un contexto en el que los cibercriminales cambian de estrategia con mayor frecuencia, optando por métodos de ataques encubiertos. Esto sucede en un momento en el que el negocio de la ciberdelincuencia supera el volumen del narcotráfico a nivel mundial, tal y como reconoce Sergio Martínez, *country manager* de SonicWall para Iberia.

Con una sutileza sin precedentes, enfocándose a objetivos concretos y vulnerando los privilegios superiores es cómo actúa una ciberdelincuencia que hace tiempo dejó atrás el "romanticismo" de unos *hackers* que actuaban en un garaje, señala el directivo. Convertidos en organizaciones muy preparadas y distribuidas, que a veces trabajan en lugares insospechados, cuentan hasta con recursos humanos y tratan de no conocerse para evitar que si uno cae, caiga toda la organización. Así es cómo define a la actual red del cibercrimen internacional Sergio Martínez.

SonicWall, compañía de ciberseguridad que se ha convertido en el segundo fabricante a nivel mundial de *firewall*, tras vender más de cuatro millones, ha detectado este año más de 465.000 variantes de *malware*. *Malware* con pequeños cambios que hacen que el dispositivo no sea capaz de detectarlo. Con su algoritmo RTDMI (Real Time Deep Memory Inspection) SonicWall observa el comportamiento y en base al mismo lo identifica. Un algoritmo al que Sergio Martínez califica como "la joya de la corona de la compañía", distinguiéndole de sus competido-

Sergio Martínez, *country manager* de **SonicWall**

SONICWALL

res al detectar *malware* que otros no son capaces de descubrir. Además, va a mejorar toda la parte de visibilidad y control con el fin de detectar los ataques, adelantándose a los mismos. Porque, tal y como señala, "si no somos capaces de detectar, ¿cómo vamos a defender?

Los datos del informe apuntan a que las cifras de *ransomware* han descendido un 21 % a nivel global y un 38 % en la región de EMEA. La realidad indica que esto sucede porque los ataques son más sofisticados, señala. Sin embargo la cantidad de ataques de *malware* hacia el IoT ha aumentado un 87 %. ¿La razón? La superficie de exposición va creciendo al contar con más dispositivos. "El *malware* de IoT es una de las grandes preocupaciones en este momento", dice, "porque la mayor parte de estos dispositivos no están controlados por el departamento de Informática. Las empresas dan móviles corporativos a sus trabajadores pero ellos tienen su móvil personal también y estos se conectan a Internet", recuerda. Al igual que ocurre en sanidad, por ejemplo, con todas las personas que pasan al día por un hospital, por lo que "o compartimentas y aíslas o estás perdido".

Futuro

El pesimismo se instala en Sergio Martínez al hablar del futuro. "Todo va a ir a peor", preconiza, algo paradójico si tenemos en cuenta que, tal y como recuerda, "estamos invirtiendo más que nunca en ciberseguridad", por lo que "algo estamos haciendo mal", reflexiona. "No contamos con los recursos requeridos porque el *gap* entre lo que necesitas y lo que tienes es a veces más grande".

Soluciones

En este momento, como siempre, su andadura irá paralela a la de las pymes. Alineados en precio y alcance tecnológico para este segmento de mercado "en el que nos sentimos muy cómodos junto a nuestro canal", confirma. "Algo que nos caracteriza es que, si tenemos un nodo de dos *firewalls*, uno trabajando y otro esperando por si

SONICWALL

este cae, licenciamos solo uno, no los dos como hace la competencia. Intentamos ponérselo fácil a la pequeña empresa. Y sobre todo trabajamos con el canal día a día, que es el departamento de informática y ciberseguridad de todas las firmas". Un canal con el que despliegan estrategias de defensa por capas, de visibilidad y control, de protección de entornos distribuidos o híbridos para detectar *malware* conocido y desconocido. "Esto último es lo que más valora el mercado frente a nuestra competencia", subraya.

En el entorno de la visibilidad SonicWall está invirtiendo en generar una plataforma mucho más potente para relacionar mejor los eventos, ofrecer reportes óptimos e ir un paso por delante de los ciberdelincuentes para que la plataforma sea capaz de detectarlo en un momento incipiente.

La compañía también invertirá en proteger la nube. Una nube que está siendo cada vez más atacada. De su solución Cloud Application Security (CAS) destaca su sencillez y puesta en marcha en tan solo minutos: "Sólo hay que dar permiso desde la herramienta que controla el *cloud*. A partir de ahí analiza el correo electrónico, los ficheros en la nube, protege las identidades, las credenciales de los usuarios, controla las conexiones extrañas…".

SonicWall también cuenta con soluciones para wifi 6 y alta velocidad. "Nuestros *access point* son soluciones basadas en wifi 6. Hemos hecho un lavado total de la gama y estamos mejorando en gran medida la administración en la nube de estos dispositivos", explica. "No son meros *access points*. Son *firewalls* en pequeño. Tienen capacidades de *firewalling* y de ciberseguridad muy avanzadas. Una capa más en la defensa por capas".

Y todo ello sin olvidar sus *switches*, "un elemento muy básico pero si quieres mas puertos en el *firewall* hay un *swicht* por lo que se puede controlar la red de manera más sencilla desde el propio *firewall*.

En la nueva era de la IA Sonicwall está presente con el bagaje que le dan sus tres décadas de experiencia en esta área, incorporándolo en todos sus dispositivos desde el *endpoint* hasta el *firewall*, pasando por el *access point,* por la protección del correo electrónico, por todas las capas… Una IA que, reconoce, puede servir a los atacantes para construir ataques mucho más sofisticados y sutiles. "Hay algoritmos que hacen cosas muy potentes. Tenemos que ser conscientes y estar preparados. Las empresas tienen que contar con copias de seguridad y tener un plan por si sufren un ataque y encriptan sus servidores, poder restaurarlos en un plazo determinado".

Recomendaciones

A la hora de proteger la red inalámbrica, Sergio Martínez recomienda añadir capacidades de ciberseguridad al *access point*. Tras esto, segmentar y desplegar estrategias zero trust porque, tal y como recuerda: "La estrategia tiene que ser de máxima confianza hacia quien se acredite a través de un *access point*, monitorizar lo que hace, obtener reportes sobre lo que está sucediendo en el mismo". Esto es fundamental para sectores como el de la educación o sanidad, añade.

SONICWALL

Plataforma de SonicWall para abordar la seguridad empresarial

Proteger a un gran número de trabajadores en remoto es algo complicado para las organizaciones en la era del trabajo híbrido. Sergio Martínez, *country manager* de SonicWall para Iberia, destaca en este vídeo que ante el entorno hostil en el que nos encontramos y en el que tan solo un 5 % de los CIO son optimistas ante la situación actual, SonicWall ayuda las organizaciones con su Plataforma de Boundless Cybersecurity. ¿Cómo? Con una defensa por capas, desde el *firewall* hasta el *endpoint*, basada en IA, protección del correo electrónico, etc. Y rodeando todo de visibilidad y control.

¿Cómo nos sorprenderá SonicWall en la era de la IA?

En esta nueva era en la que la IA marcará el futuro, SonicWall se posiciona como pionero en utilizar la IA en el panorama de la ciberseguridad pero ¿con qué nos sorprenderá? Con algo que viene haciendo desde siempre: detectando las nuevas variantes de *malware* y protegiendo a las organizaciones a través de una defensa por capas desde el *firewall* hasta el *endpoint*, tal y como apunta en este vídeo Sergio Martínez, *country manager* de SonicWall para Iberia.

Zyxel, el ángel custodio que protege a las pymes con una seguridad simplificada

"Las pymes ya no ven la ciberseguridad como un gasto, sino como una inversión". Esta afirmación de Gonzalo Echeverría, *country manager* de Zyxel Iberia, es el mejor reflejo de la evolución que ha experimentado la ciberseguridad en los últimos tiempos. Un proceso que, como explica, ha sido especialmente significativo entre las pequeñas y medianas empresas porque "eran las que mayor margen de mejora tenían y a las que todavía les queda mucho camino por recorrer" en este ámbito.

Gonzalo Echeverría, *country manager* Iberia de **Zyxel**

En este cambio de mentalidad, la concienciación sobre el papel fundamental de la ciberseguridad en un negocio, el ser conscientes de que les pueden atacar igual que a las grandes corporaciones y el miedo a que se vean obligadas a parar su negocio durante horas, días o, incluso, semanas, con el impacto negativo que esto puede ocasionales, han empujado a las pymes a invertir en seguridad. Unas inversiones que, como apunta el directivo, "deben hacerse teniendo en cuenta el tamaño de la empresa".

Pero no solo el tamaño de la compañía rige la inversión, también lo hacen las diferentes necesidades que tienen los empleados. En este sentido, y como explica Echeverría, "las pymes ya son conscientes de que necesitan una seguridad a nivel usuario y a nivel dispositivo y que, además, deben establecer distintos niveles de seguridad dependiendo de los requerimientos de los trabajadores". Labor que con los *firewalls*

EDITORIAL
SUMARIO
CHECK POINT SOFTWARE
FLEXXIBLE
SONICWALL
ZYXEL

ZYXEL

de Zyxel es una tarea sencilla ya que "les permiten crear niveles a través de la creación de perfiles y jerarquías", afirma. De esta simple manera las pymes consiguen establecer diferentes capas de seguridad para conseguir un nivel de protección máximo.

Siempre al lado de la pyme

Las habilidades digitales son otro de los puntos fundamentales actualmente. Conocer las herramientas con las que se trabaja y sacarles el mayor rendimiento posible es una máxima. Para conseguirlo la formación es clave y, por supuesto, la concienciación. "El nivel de seguridad de una empresa va a estar marcado por el usuario con el nivel más bajo, por ello la formación y concienciación son fundamentales", asegura el responsable del negocio de Zyxel Iberia.

Además, para garantizar la mayor protección, a pesar de la baja concienciación o mala praxis de los trabajadores, "los fabricantes tenemos que ofrecer un servicio capaz de detectar y parar cualquier amenaza en caso de que los usuarios no lo hagan". Unas herramientas que, como explica Echeverría, aíslan el elemento sospechoso en una red externa y lo examinan con el fin de averiguar si es un caso de *malware* o no.

Una máxima, la protección de las pymes a través de soluciones sencillas, que dibuja la hoja de ruta de Zyxel, la cual ha ido cambiando para adaptarse a las nuevas necesidades de estas empresas. Nuevos requerimientos que se han ido dirigiendo hacia la gestión remota y las líneas de *backup*. Sobre el primer aspecto, el directivo indica que "la pyme, a pesar de ser pequeña, necesita tener acceso en todo momento a la gestión de su red, visibilidad y monitorización". Mientras que las líneas de *backup* responden a la necesidad de tener la seguridad de que, en caso de que la línea principal de Internet se caiga, podrán seguir trabajando. "Actualmente las pymes tienen gran cantidad de servicios basados en la nube y con la tecnología 5G somos capaces de garantizarles seguir funcionando, aunque la red principal se haya caído", explica.

Gracias a los *router* 5G, Zyxel ofrece al segmento pyme la oportunidad de tener una línea de

ZYXEL

"A las pymes hay que ofrecerles soluciones que les permitan, de una forma sencilla, conseguir el máximo nivel de seguridad"

respaldo que salta en caso de que la principal tenga problemas. De esta manera, las empresas pueden seguir funcionando y elegir cuáles de sus servicios, ya sean básicos o críticos, seguirán operativos para dar cobertura a sus clientes.

Echeverría asegura que este servicio está en pleno crecimiento y que la compañía espera que, en los próximos años, gracias a la llegada del 5G, "crezca aún más".

Otra apuesta clara de las pymes hoy en día está siendo el ancho de banda ya que, como indica el directivo, puede marcar la diferencia respecto a la competencia. Beneficio del que las pymes cada vez son más conscientes. Unas demandas que están influyendo en los planes de Zyxel, pero que, a su vez, están ayudando a la compañía a diseñar y proporcionar una oferta cada vez más completa y especializada para el segmento pyme.

Oteando el horizonte

Autenticación. Esta es la clave que, según Echeverría, va a marcar el mercado de la ciberseguridad en la segunda parte del año y, especialmente, el 2024. "Antes había que preservar el dato, pero ahora las empresas tienen que asegurarse de que el dispositivo y el usuario son quienes dicen ser", subraya el directivo.

Un aspecto en el que la pyme tiene "una enorme vulnerabilidad" porque, si carece de los sistemas necesarios, para los ciberdelincuentes es muy sencillo suplantar la identidad de alguno de los empleados para robar información o en-

ZYXEL

criptarla y poder pedir un rescate. Por ello, en Zyxel están trabajando para proporcionar a las pymes soluciones y servicios que les garanticen "tener el máximo nivel de seguridad" y que ofrezcan un control de acceso seguro.

En cuanto al papel que están jugando, y seguirán jugando, los fondos NextGenerationEU en la mejora del nivel de seguridad de las pymes, Echeverría se muestra convencido de que, de aquí a finales de 2024, cuando el programa Kit Digital finalice, "el nivel de ciberseguridad en las pymes habrá mejorado, pero no gracias a los fondos".

El directivo cree que "los fondos europeos representan una oportunidad enorme siempre y cuando se articulen correctamente". Hecho que, como explica, no está siendo fácil y está provocando que sea un proceso engorroso, no tanto para la propia pyme, sino para el canal de distribución, que es en la figura en la que está recayendo la responsabilidad.

En cuanto a cómo será la marcha del negocio para Zyxel Iberia, Echeverría indica que la compañía cerrará el año con un crecimiento superior al 30 % y que las previsiones para 2024 apuntan a un crecimiento por encima del 20 %.

Unos datos positivos para la filial ibérica que, como comenta su responsable, se deben, por un lado, a que "nos dirigimos a un segmento cuyo potencial de crecimiento es todavía mucho mayor que en el resto de segmentos empresariales". Y, por otro lado, gracias a que "tenemos una nueva gama de productos más específica y centrada en las demandas actuales de las pymes".

De la protección del dato a la del acceso

Gonzalo Echeverría, *country manager* de Zyxel Iberia, explica cómo las pymes han pasado de buscar herramientas que garanticen la seguridad perimetral a soluciones que protejan los dispositivos y usuarios. Para garantizar la máxima protección, tanto en la oficina como fuera de ella, las empresas están apostando por *firewalls* de nueva generación. Unas herramientas que, como asegura el directivo, "ofrecen la mejor conectividad con el máximo nivel de seguridad para todos los dispositivos y usuarios". Porque "antes había que proteger el dato, pero ahora es necesario proteger la identidad", subraya.