ciberseguridadTIC
seguridad en informática y comunicaciones
Tai editorial
Año I Nº 1
Febrero 2023

Innovación al servicio de la seguridad

Iberdrola:
"De cara a futuro va a ser muy importante la convergencia de tecnologías"

Cerealto:
"La ciberseguridad no es *plug&play*, hay que trabajarla mucho"

Elastic:
"Elastic se ha introducido en el mundo de la seguridad con una aproximación XDR"

Ciberseguridad, un mercado en constante evolución

El mercado de ciberseguridad es uno de los más dinámicos. Constantemente aparecen nuevos conceptos, nuevas siglas, nuevos espacios que los ciberdelincuentes pueden explotar. Y aparecen nuevos medios de comunicación, como el que está leyendo en estos momentos.

Ciberseguridad TIC nace de la experiencia y de la pasión por un mercado en constante evolución, transversal e imprescindible para hacer frente al día a día tecnológico.

En este primer número hablamos de innovación. Lo que parecía conseguido, aún está lejos de estarlo, y quizá no tenga importancia ponerle un nombre nuevo a lo que ya se lleva haciendo desde hace tiempo en modo anónimo, pero las siglas van apareciendo y, estemos más o menos de acuerdo, mejor tener los conceptos en el radar.

Además, nos acompañan en el lanzamiento diferentes expertos, de uno y otro lado. En el juego del gato y el ratón van en el mismo equipo, haciendo frente a ciberataques cada vez más sofisticados. Unos están en primera línea de batalla, tomando decisiones a vida o muerte; los otros ocupan su posición en retaguardia, en un constante desarrollo de productos y tecnologías que ayuden a ganar la guerra.

El principal reto de los primeros es la complejidad, el tratar con cada vez más capas tecnológicas que gestionan en un puro equilibrio. Su mayor demanda, la simplicidad. Es el mercado el que tiene que responder.

Muchas gracias a todos por acompañarnos.

SUMARIO

Directora:
Rosalía Arroyo
rosalia@taieditorial.es

Publicidad:
David Rico
david@taieditorial.es

Producción:
Marta Arias
marta@taieditorial.es

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

Innovación al servicio de la seguridad

El mercado de seguridad es uno de los más dinámicos. No solo innova para sí mismo, sino para proteger las innovaciones tecnológicas que se gestan en otros entornos, como el de desarrollo, almacenamiento o comunicaciones.

Este dinamismo es lo que impulsa nuevas tendencias, nuevos conceptos... y nuevas siglas. Ya no se habla de CASB, ahora es SASE, o SSE si me apuras; ya no es CSPM, ahora hablamos de CNAPP; y la detección y respuesta se añade a todo, desde el *endpoint*, a la red o, lo último, a la amenaza de identidades. Acompáñanos en este artículo en el que daremos un repaso por algunas tendencias del mercado de ciberseguridad.

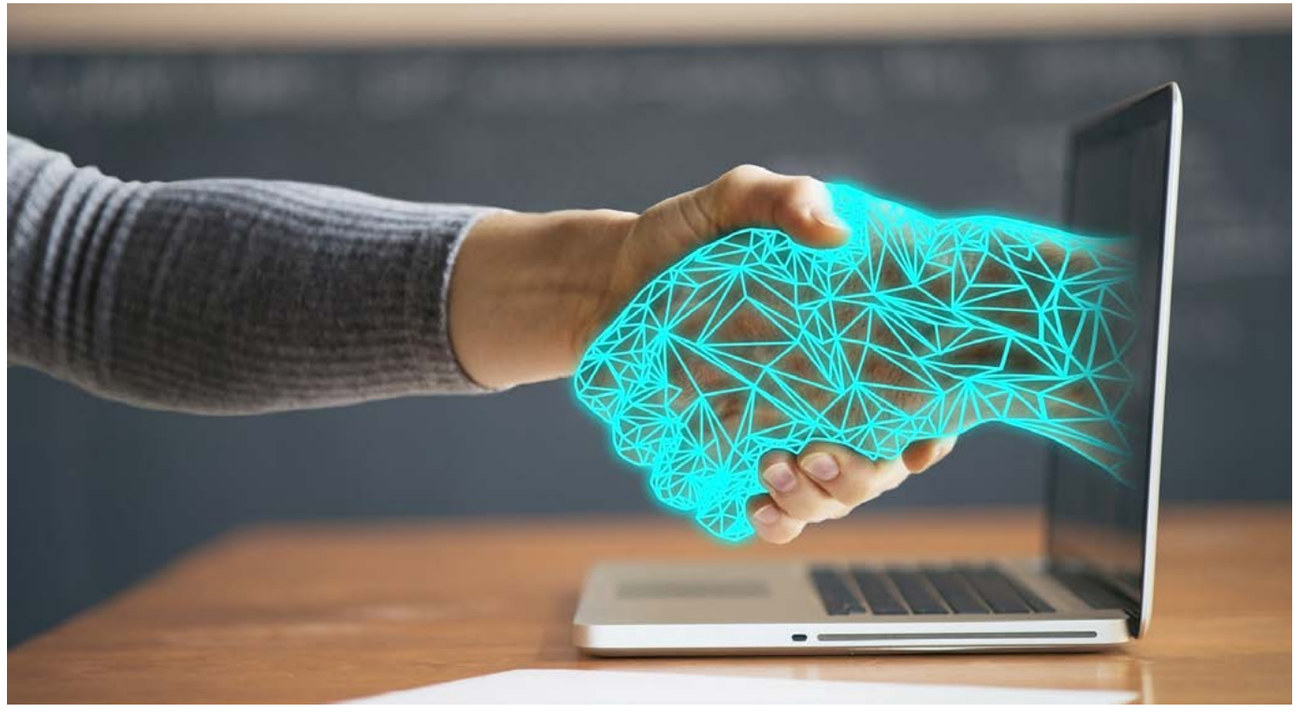
EN PORTADA

De CASB a SSE

Hace una década, cuando el mercado se había convencido de que la migración al *cloud* era solo cuestión de tiempo, apareció el término CASB (Cloud Access Security Management), que buscaba dar visibilidad a lo que estaba ocurriendo en la nube y hacer cumplir con las políticas de seguridad. No solo permitía saber a las empresas cuántas aplicaciones tenían en la nube, dando luz al famoso *Shadow IT*, sino tener control sobre las actividades del usuario y los datos confidenciales.

Bajo el concepto CASB aparecieron muchas empresas, y a su alrededor se produjeron importantes movimientos de consolidación. En pocos años muchos grandes se quedaron con jóvenes empresas, sin que los detalles financieros de todos los acuerdos trascendieran:

- En septiembre de 2015 Microsoft compró Adallom por 250 millones de dólares.
- En julio de 2015 Blue Coat compró Perspecsys, y meses más tarde se haría con Elastica por 280 millones de dólares. Por cierto, que Symantec compraría Blue Coat en 2016 por 4.650 millones de dólares.



El 80 % de las brechas de seguridad involucran el uso de credenciales privilegiadas

- En julio de 2026 Cisco pagó 293 millones de dólares por CloudLock.
- En octubre de 2016 Proofpoint compró FireLayers.
- En febrero de 2017 Forcepoint compró Skyfence por 40 millones de dólares.
- En septiembre de 2017 Oracle compró Palerra.
- En noviembre de 2017 McAfee compró Skyhigh Networks.

EN PORTADA

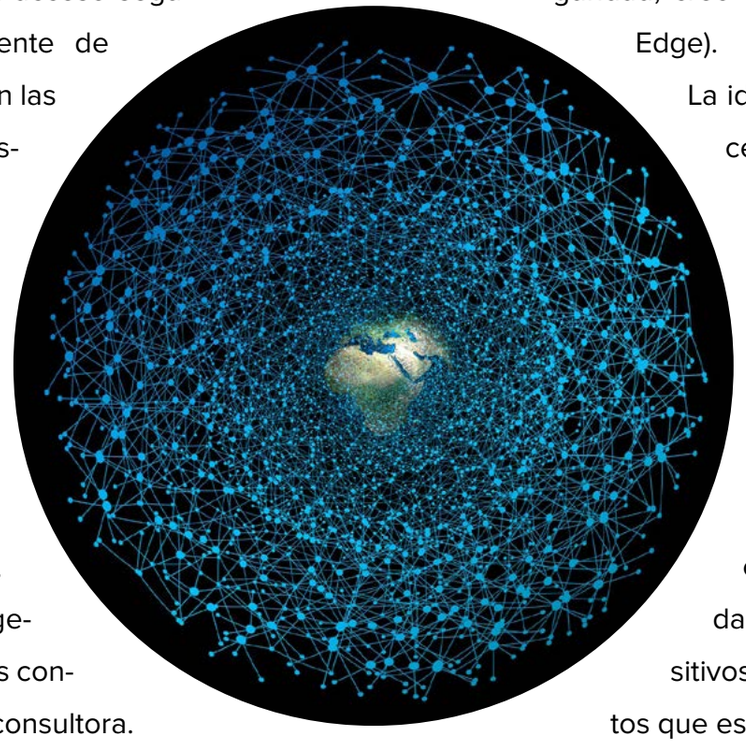
Terminados estos tres años de compras casi compulsivas quedaron en el mercado Netskope, Bitglass y CipherCloud. Las dos últimas fueron adquiridas en 2021. Forcepoint compró Bitglass y Lookout compró Cipher Cloud.

Y el tiempo fue pasando, y fueron apareciendo nuevos jugadores, y el concepto CASB empezó a caer en desuso, dando lugar al SASE (Secure Access Service Edge), que ha despertado pasiones y creado un grupo de férreos seguidores, los *SASE Believers*.

CASB es una herramienta que se ubica entre los usuarios y un servicio en la nube para hacer cumplir las políticas de seguridad en torno a los recursos basados en la nube, y ayuda a las empresas a detectar actividades inusuales o maliciosas y administrar mejor el acceso a la nube con visibilidad profunda y control granular.

SASE se basa en los cimientos de CASB, pero aborda las necesidades de seguridad de red más amplias de las empresas. Combina redes de área amplia definidas por software (SD-WAN) con seguridad de red completa, lo que aumenta la seguridad, mejora el rendimiento de la red y reduce los costos. Cuando se implementa correctamente, SASE permite a las empresas aplicar un acceso seguro independientemente de dónde se encuentren las aplicaciones, los dispositivos, los usuarios y las cargas de trabajo, lo cual es vital para las fuerzas de trabajo remotas.

La última vuelta de tuerca la dio Gartner, una de las mejores generadoras de nuevos conceptos, además de consultora. Gartner fue, de hecho, quien acuñó el término SASE en 2019, y quien, a finales de 2021, en respuesta a la evolución del mercado de seguridad, creó SSE (Secure Service Edge).



La idea de SASE es ofrecer una arquitectura de seguridad más dinámica y descentralizada que las arquitecturas de seguridad de red tradicionales, ya que tiene en cuenta la gran cantidad de usuarios, dispositivos, aplicaciones y datos que están localizados fuera

> Lo habitual es que CSPM sea utilizado por organizaciones que han adoptado una estrategia *cloud-first*

Las CNPP también incorporan la gestión de derechos de identidad; seguridad de automatización y orquestación, particularmente para *kubernetes* y detección y protección de API

del perímetro de la empresa. SASE ofrece un enfoque flexible y "en cualquier lugar, en cualquier momento" para proporcionar acceso remoto seguro mediante la entrega de múltiples capacidades, incluida la puerta de enlace web segura (SWG) para proteger los dispositivos de las amenazas basadas en la web; agente de seguridad de acceso a la nube (CASB), que actúa como intermediario entre los usuarios y los proveedores de la nube para garantizar el cumplimiento de las políticas de seguridad; cortafuegos de última generación; y acceso a la red de confianza cero (ZTNA), que considera el contexto, como la identidad, la ubicación y el estado del dispositivo, antes de otorgar acceso remoto a las aplicaciones.

Una forma sencilla de entender SSE, frente a SASE, es que el primero desacopla los elementos de seguridad primarios de la parte de red (es decir, el *firewall*) de SASE. El informe del Cuadrante Mágico de Gartner señala a SWG, CASB y ZTNA como los componentes necesarios de una oferta completa de servicios de seguridad.

De CSPM a CNAPP, pasando por CIEM y CWPP

CSPM (Cloud Security Posture Management), o gestión de la postura de seguridad del *cloud* hace referencia a las herramientas de seguridad que están diseñadas para identificar los problemas de mala configuración y cumplimiento en la nube. Un problema que parecería baladí si no fuera porque varios estudios identifican los errores de configuración como uno de los principales problemas de seguridad asociados a la nube.

CSPM también es un término acuñado por Gartner, y uno de sus principales objetivos es monitorizar de manera continua la infraestructura de la nube en busca de brechas en la aplicación de políticas de seguridad. Según la consultora, el uso de una herramienta CSPM puede reducir los incidentes de seguridad basados en la nube debido a configuraciones incorrectas en un 80 %.

Lo habitual es que CSPM sea utilizado por organizaciones que han adoptado una estrategia *cloud-first* y desean extender sus mejores prácticas de seguridad a entornos de nube híbrida y *multicloud*.

Las herramientas de CSPM funcionan examinando y comparando un entorno de nube con un conjunto definido de mejores prácticas y riesgos de seguridad conocidos. Algunas he-

Combatiendo las nuevas ciberamenazas

Al margen de siglas y palabros, que no hacen sino bautizar tendencias con nombres más o menos atractivos, lo que está claro es que los ciberataques han aumentado, tanto en número como en sofisticación.

La firma McKinsey examinó hace unos meses tres de las últimas tendencias en ciberseguridad y sus implicaciones para las organizaciones. Tendencias que siguen de plena actualidad.

1. Acceso bajo demanda a las plataformas de datos e información

Las organizaciones recopilan muchos más datos sobre los clientes, desde transacciones financieras hasta consumo de electricidad y vistas en las redes sociales, para comprender e influir en el comportamiento de compra y pronosticar la demanda de manera más efectiva. Las empresas no solo recopilan más datos, sino que también los centralizan, los almacenan en la nube y otorgan acceso a una variedad de personas y organizaciones, incluidos terceros, como proveedores.

2. Uso de IA y ML en los ciberataques

El ciberdelincuente que trabaja solo ya no es la principal amenaza. Hoy en día, el cibercrimen es un negocio que mueve miles de millones de dólares, que se organiza en empresas, trabaja con presupuestos y también destina fondos al I+D.

Los ciberdelincuentes utilizan herramientas avanzadas, como inteligencia artificial, aprendizaje automático y automatización. Durante los próximos años, podrán acelerar, de semanas a días u horas, el ciclo de vida del ataque de extremo a extremo, desde el reconocimiento hasta la explotación.

3. Regulaciones, brechas y falta de personal

Muchas organizaciones carecen de suficiente talento, conocimiento y experiencia en ciberseguridad, y el problema va en aumento. Muchas empresas no están seguras de cómo identificar y gestionar los riesgos digitales, y para agravar el desafío, los reguladores están aumentando la presión con nuevas normativas.

rramientas CSPM alertarán al cliente de la nube cuando sea necesario remediar un riesgo de seguridad, mientras que otras herramientas CSPM más sofisticadas utilizarán la automatización de procesos robóticos (RPA) para remediar los problemas automáticamente.

De manera genérica, las características clave de las herramientas empresariales de administración de postura de seguridad en la nube más habituales incluyen la capacidad de detectar y quizás remediar automáticamente configuraciones incorrectas de la nube; mantener un inventario de mejores prácticas para diferentes configuraciones y servicios en la nube; mapear los estados de configuración actuales a un mar-

co de control de seguridad o estándar regulatorio; y trabajar con plataformas IaaS, SaaS y PaaS en entornos de nube híbrida y multinube en contenedores.

En los últimos tiempos, CSPM está perdiendo fuelle a favor de CNAPP (Cloud Native Application Protection Platform), que no puede ser entendido si no mencionamos antes el CWPP (Cloud Workload Protection Platform), una plataforma de protección de la carga de trabajo en la nube que supervisa automáticamente una amplia gama de cargas de trabajo, incluyendo servidores físicos locales, máquinas virtuales y funciones sin servidor; CIEM (Cloud Infrastructure Entitlements Management), encargados de gestionar identidades y privilegios de acceso en entornos de nube y multinube; o IAM (Identity Access Management) para la gestión de accesos e identidades. La CNAPP constituye una nueva categoría de plataforma de seguridad en la nube que consolida CSPM, CIEM, IAM, CWPP, protección de datos y otras capacidades.

Es decir, CNAPP combina varias áreas tecnológicas. En estas plataformas convergen la seguridad de la carga de trabajo en la nube con (CWPP) y la seguridad de la configuración (CSPM) para el plano de control de la nube, que ya están cubiertas por las plataformas de protección de la carga de trabajo en la nube (CWPP) y la gestión de la postura de seguridad en la nube (CSPM). Las CNPP también incorporan la gestión de derechos de identidad; seguridad de automatización y orquestación, particularmente para *kubernetes*; y detección y protección de API.

ITDR

También acuñado por Gartner, ITDR (Identity Threat Detection and Response) es una nueva categoría de seguridad diseñada explícitamente para proteger las identidades y los sistemas que las administran.

ITDR (Identity Threat Detection and Response) es una nueva categoría de seguridad diseñada explícitamente para proteger las identidades y los sistemas que las administran

Los ataques a la capa de identidad han aumentado en los últimos dos años debido a la mayor adopción del trabajo remoto y de la nube. De hecho, según datos del Verizon Data Breach Investigations Report, el 80 % de las brechas de seguridad involucran el uso de credenciales privilegiadas.

La amenaza contra las identidades ha llevado a un floreciente mercado en torno a la gestión de identidades y clientes, así como la mayor adopción de herramientas de autenticación como MFA y SSO, todo ello destinado a administrar nuestras identidades de la manera más efectiva y reducir las posibilidades de credenciales comprometidas. Hay que entender el ITDR como la colección de herramientas y mejores prácticas para defender los sistemas de identidad.

En esencia, ITDR detecta el robo de credenciales y el uso indebido de privilegios, los ataques a Active Directory y los derechos de riesgo que crean rutas de ataque. A diferencia de las herramientas de protección de identidad existentes, como IAM, PAM o IGA, que se centran en la autorización y la autenticación, las soluciones de ITDR protegen las identidades, los derechos y los sistemas que los gestionan, lo que garantiza que las personas adecuadas tengan acceso a los recursos que necesitan. ITDR proporciona visibilidad del uso indebido de credenciales, exposiciones de derechos y actividades de escalada de privilegios, que se extienden desde el punto final hasta AD y entornos de múltiples nubes.

Iberdrola: “De cara a futuro va a ser muy importante la convergencia de tecnologías”

Hablamos con Luis Villafruela, Responsable Ciberseguridad TI de Iberdrola, para quien saber qué ingredientes tienen que componer tu plato principal, y cómo adaptarlo a tu contexto, es clave a la hora de seleccionar una tecnología concreta en un mercado con demasiada oferta; que prefiere centrase en procesos de TI bien reforzados, más que hablar de tecnologías de seguridad básicas; para quien la protección de la carga de trabajo es muy relevante y quien espera una evolución en el control de seguridad en entornos *cloud*.

Luis Villafruela,
Responsable Ciberseguridad TI de **Iberdrola**

Habituado a ser gestor del área de TI clásica, la ciberseguridad había tocado “un poco de lado” a Luis Villafruela, que se movía a sus anchas en el mundo del desarrollo y la arquitectura de sistemas. A lo largo de su dilatada carrera, el responsable de Ciberseguridad TI de Iberdrola también ha tenido que hacerse cargo de la provisión de servicios de Internet, lo que le ha permitido tener “una visión muy clara y muy madura de cómo deben ser los procesos de TI”.

Dice también el directivo de Iberdrola que su capacidad de adaptación le sirvió para adentrarse en el mundo de la ciberseguridad cuando llegó la oportunidad “de potenciar una función nueva que se iba a asentar sobre ese mapa de procesos de la gestión de TI clásica. La ciberseguridad”. Reconoce que no la fue buscando, sino que la ciberseguridad se fue poniendo en

> "Más que hablar de herramientas, apostaría por procesos de TI bien reforzados"

su camino, convirtiéndole en experto en gestión de riesgos, planes estratégicos, orquestación de soluciones... hasta nuestros días. Días en los que la ciberseguridad es un área muy demandada, que genera mucha visibilidad en la alta dirección, y cuya evolución "ha sido muy significativa". Dice Luis Villafruela que ser un buen gestor de riesgos de ciberseguridad es una de las primeras cualidades que debe tener un buen responsable de ciberseguridad, explicando que en una empresa tan grande como Iberdrola hacer una buena gestión de riesgos es una tarea muy compleja para lo que se necesita conocer muy bien la empresa, saber identificar los activos críticos de la compañía y cuáles son sus procesos más relevantes.

Un buen CISO, además, tiene que ser una persona con mucha capacidad en la organización y tener una buena agenda porque "el *networking* es muy importante para estar coordinados con otros responsables de ciberseguridad, *partners*, fabricantes". Añade como cualidad el estar muy preocupado por las personas y los procesos, porque "son dos áreas muy relevantes en la agenda de un CISO", más incluso que la tecnología porque, como asegura el responsable de ciberseguridad TI de Iberdrola "hay tanta tecnología que es imposible que uno sea un súper experto en todo".

La ciberseguridad empieza a verse como una inversión, al menos en empresas grandes, dice Villafruela cuando le preguntamos si la ciber-

ENTREVISTAS

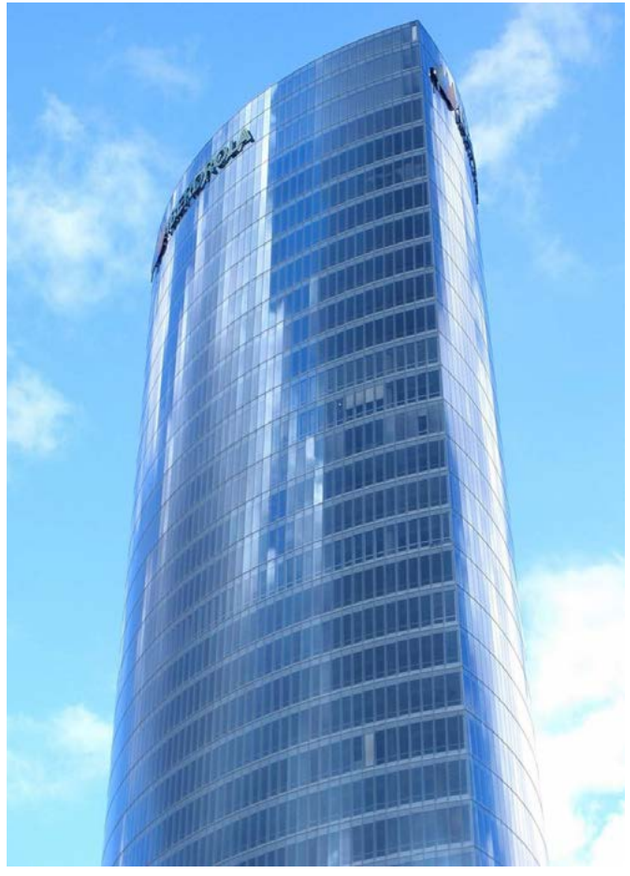
> "Los CSPM tiene que evolucionar bastante y en los próximos dos años deberían dar un paso adelante para poder orquestar la postura a ese nivel"

seguridad empieza a dejar de verse como un gasto. "Es una inversión, y si no inviertes lo suficiente al final seguro que vas a pagar más con los ciberataques", comenta el directivo.

"Saber qué ingredientes tienen que componer tu plato principal y cómo adaptarlo a tu contexto", es clave a la hora de seleccionar una tecnología concreta en un mercado con demasiada oferta. Explica Luis Villafruela que hay tantos fabricantes y tantas soluciones que "muchas de ellas pueden ser buenas o no dependiendo de qué procesos tengas, cómo los tengas organizados, cuál es el contexto de tu negocio, tu posicionamiento estratégico o las ciberamenazas que pueda tener tu propio sector". Asegura también que se ha convertido en un reto poder elegir buenas soluciones porque, cuando el mercado ha visto que se estaban haciendo grandes inversiones, todos, grandes y pequeños, se han lanzado a proporcionar soluciones de seguridad, lo que ha generado un problema: "tener demasiadas soluciones que además no se hablan correctamente". La situación lleva al responsable de ciberseguridad TI de Iberdrola a asegurar que, "de cara a futuro, va a ser muy importante la convergencia de tecnologías, o al menos la compartición de tecnologías en ciertas plataformas multifabricante para eficientar esos procesos de ciberseguridad. Si no, va a ser imposible".

Amenazas

El ransomware es una de las amenazas según Luis Villafruela. También preocupa el phishing, junto con la seguridad de la cadena de suministro, que está llevando a reforzar toda la gestión de los contratos con los proveedores más importantes y aquellos que "te ayudan a soportar los procesos más críticos de negocio, con los que hay que mantener una postura de seguridad con unos estándares muy altos".



ciberseguridadTIC

tai editorial

ENTREVISTAS

> "El empleado es el activo más importante de la empresa y lo tienes que proteger como a todo lo demás"

De manera más genérica hace referencia el responsable de ciberseguridad TI de Iberdrola a la ciberdelincuencia patrocinada por estados como otra de las amenazas que están en el radar de su compañía.

¿Qué peso crees que tiene la concienciación del usuario en la seguridad empresarial? "Mucha, porque el empleado es el activo más importante de la empresa y lo tienes que proteger como a todo lo demás", dice el directivo, añadiendo que la concienciación es muy importante ya que, además, "los empleados crean una red de sensores y si están bien concienciados incluso te pueden avisar de ciertas situaciones".

Especializado en Inteligencia Artificial en la Universidad de Informática, dice Luis Villafruela que, aunque en aquellos tiempos sólo era listilla, ahora es verdaderamente inteligente, "para lo bueno y para lo malo".

Tecnologías

Preguntado por las tecnologías de seguridad básicas que debería tener cualquier empresa con un presupuesto mínimo, empezaría el directivo de Iberdrola por un antivirus clásico con EDR. A continuación, más que hablar de herramientas, "hablaría de procesos de TI bien reforzados". Tiene claro Villafruela que es necesario tener un buen inventario para saber cuál es tu superficie de ataque y hacer una gestión de riesgos mínima; menciona de manera concreta los procesos de gestión de las infraestructuras y de las bases de datos, y de tener muy bien controlado la obsolescencia de tu hardware y el software de base de datos; un buen parcheo y un cierto nivel de bastionado seguro de esas infraestructuras". Difícil no añadir "algo de monitorización, un SIEM básico y alguna herramienta de orquestación de incidencias de seguridad".

ENTREVISTAS

> "El *networking* es muy importante para estar coordinados con otros responsables de ciberseguridad, *partners*, fabricantes"

Las empresas más pequeñas accederán a muchos de estos mínimos a través de servicios gestionados, aunque hay una parte que no puedes delegar, que es "la relacionada con la identificación y gestión de riesgos, porque no es lo mismo una empresa de distribución, que una energética, una aerolínea o una empresa de hoteles. Cada una tiene su punto focal en un sitio".

El gobierno de las identidades en un ecosistema de tantas personas trabajando en proyectos y servicios, "es una cosa básica", responde Luis Villafruela cuando le preguntamos por tecnologías que serán necesarias en un futuro cercano, si no es que lo son ya. "No solo gestión de identidades, sino gobierno, segregación de responsabilidades y una monitorización continua de que están bien segregados los roles y no tienes interferencias", apunta el directivo.

Junto a la gestión de usuarios, la de credenciales, que para Luis Villafruela "es un *must* en el corto plazo".

Otra área importante es un "XDR de verdad, operativo". Asegura que "hasta ahora hemos estado hablando mucho de XDR, pero falta un poco para asentarlo de verdad". Se necesita, asegura, "una buena solución de XDR con una telemetría totalmente integrada, utilizando Inteligencia Artificial para correlar todo tipo de eventos, y por supuesto un *partner* que te de ciberinteligencia no sólo de tu contexto, sino de todos los clientes que tenga alrededor del mundo. Eso es muy relevante". Es decir, que se apuesta por la ciberinteligencia.

Espera también el directivo de Iberdrola "una evolución en todo lo que es el control de la pos-

tura de seguridad en entornos *cloud*". Asegura que los CSPM tiene que evolucionar bastante "y en los próximos dos años deberían dar un paso adelante para poder orquestar la postura a ese nivel".

Añade como tecnologías imprescindibles en el futuro cercano las soluciones de desarrollo seguro asegurando que "la protección del workload es muy relevante porque todos los desarrollos son ágiles, tienen que ir al mercado rápido, tienen que entrar en producción muy rápido, y esa es otra de las áreas que hay que industrializar muy bien dentro del proceso de desarrollo seguro".

A más largo plazo apuesta Villafruela por la integración IT OT, "como una de las áreas que vemos en el radar".

La guerra de Ucrania, donde se ha hecho evidente el impacto que pueden tener los ciberataques en los conflictos bélicos, y de manera específica contra las infraestructuras críticas, "ha venido a reforzar la concienciación de la alta dirección en asumir que la ciberseguridad es una buena inversión". Además, "al ser infraestructura crítica, se está poniendo mucho foco también en la ciberseguridad en entornos OT".

ENLACES DESTACADOS

Stormshield: "Los fabricantes debemos hacer un esfuerzo por facilitar el uso y el acceso a tecnologías de seguridad"

"En el ámbito de la seguridad de la información toda colaboración y toda coordinación es poca. Nadie sobra" (Microsoft)

ciberseguridadTIC

TAI editorial

“La ciberseguridad no es *plug&play*, hay que trabajarla mucho”

Tiene claro Juan Manuel García Dujo, CIO y CISO de Cerealto, que no hay que caer en el error de vender miedo, que es mejor explicar los riesgos; que un buen CISO tiene que tener capacidades técnicas, y también de negocio; que es mejor tener menos cosas, pero bien montadas, y pocos proveedores, pero de gran confianza; y que lo que necesita el mercado es “tecnologías que nos hagan la vida más sencilla”.

Juan Manuel García Dujo, CIO y CISO de **Cerealto**

Que el mundo de la seguridad esté unido al mundo de la tecnología, y además te guste, fue el caldo de cultivo para que Juan Manuel García Dujo, actualmente CIO, CISO, DPO y algunas otras cosas más, de Cerealto Siro Foods diera un paso al frente cuando, hace cerca de 10 años, su compañía se planteara crear un departamento de Seguridad de la Información, que arrancaría de cero y dependería del Departamento de Sistemas. Recuerda el directivo que poco a poco aquello fue creciendo y en dos o tres años “ya había dos personas e incluso se empezaba a hablar de ciberseguridad industrial”.

En opinión de García Dujo la ciberseguridad ha dejado de ser “algo que hay que tener, a algo que aporta valor a la compañía”, y asegura que ha sido un reto “que el chico que siempre dice no pueda decir cómo sí hacerlo, y se le tenga en cuenta”. Con el tiempo, aquel Departamento de la Información fue creciendo, aumentando la responsabilidad, “y ahora compagino los dos roles, CIO y CISO que, aunque no sea el ideal, sí que tiene sentido”. Al final, sobre Juan Manuel García Dujo, recaen las labores de Director de Transformación Digital (CIO & CISO), DPO y Ciberseguridad OT.

ciberseguridadTIC

TAI editorial

ENTREVISTAS

> "Que el chico que siempre dice no pueda decir cómo sí, y se le escuche, ha sido un reto"

Cualidades

"Ser capaz de aunar dos mundos" es una de las cualidades que debe tener un buen CISO. Habla García Dujo de capacidades técnicas y de negocio, y de empatía y actitud, y asegura que la más importante es tener una visión tecnológica transversal de toda la infraestructura de la compañía, incluidas las comunicaciones, aplicaciones, servidores, desarrollo de aplicaciones, el mundo de internet, el *cloud*... y con una especialización en alguna de estas áreas, porque "si sabes las tecnologías, sabes cómo protegerlas".

El tener visión de la parte de seguridad física aporta valor, porque se tiene una foto de 360 grados de la seguridad integral de una compañía. Además, la seguridad física favorece la relación con las Fuerzas de Seguridad del Estado que es muy valiosa "porque al final todos los CISO acabamos teniendo incidentes de uno u otro tipo que pueden acabar en una denuncia, en un proceso con las fuerzas de seguridad del Estado, con lo cual es bueno saberte relacionar con ellos y es una de las capacidades que se tienen que tener".

Menciona también el CISO de Cerealto Siro Foods que es conveniente contar con" una capa legal para estar al tanto de todas las directivas que afectan a la compañía a la que se sirve. Debes conocer qué base legal tienes cuando haces monitorización de datos, o conocer el lenguaje que habla el equipo legal de la compañía", apunta, como otra de las cualidades de un buen CISO.

En cuanto a las habilidades menos técnicas, habla Juan Manuel García Dujo de "visión del

negocio de la compañía en la que estás porque la compañía vive del negocio, no vive de la seguridad, la seguridad es un habilitador más para el negocio". A esto se suma el contar con habilidades de comunicación, porque hay que saber explicar la seguridad a toda la compañía y hacer pedagogía, "sin caer en el error de vender miedo. A mí no me gusta vender miedo. Creo que es mejor explicar los riesgos y hacerles conscientes de ellos explicándoselos en un lenguaje que entiendan".

Finalmente hay dos palabras que, en opinión de este directivo, deben acompañar al CISO: confianza y templanza.

Seguridad y Amenazas

Poco a poco la seguridad está pasando de ser un gasto, una necesidad, a un elemento que aporta valor a la compañía. Va García Dujo un paso más allá, y habla del riesgo de que se convierta en una *commodity*; "puede que en ciertos casos estemos llegando a ser un *commodity*, lo cual es un riesgo" porque "no por comprar la mejor caja, ponerla y enchufarla va a funcionar y voy a ser más seguro. La ciberseguridad hay que trabajarla mucho. No es *plug&play*".

Preguntado sobre cómo se escoge una solución de seguridad en un mercado plagado de fabricantes y propuestas, comentar el CIO y CISO de Cerealto Siro Foods que la ciberseguridad se ha convertido en una moda, que la mayoría de los proveedores del mercado tienen servicios de ciberseguridad y que "es imposible que todos sean buenos". Igual que ocurre con la capa tecnológica, el boca a boca entre compañeros es bueno, sigue funcionando "y te ayuda a hacer un primer filtro".

En todo caso, apuesta el directivo por "tener pocas cosas, pero bien montadas; pocos proveedores, pero de gran confianza. El menos es más es otra de las reflexiones en este momento".

¿Qué amenaza le quita el sueño a Juan Manuel García Dujo? "Lo más crítico es una parada de producción, que es cierto que puede venir de mil cosas, desde un *ransomware* a una brecha

de seguridad o un problema en un proveedor", responde el entrevistado.

Concienciación y tecnología

En Cerealto conviven dos mundos, el industrial, con sus procesos, que están interconectadas con el mundo IT, y el mundo del mundo oficina. En ambos, "la concienciación es algo fundamental" porque el usuario es la primera persona que puede parar un ataque. Pero eso sólo va a pasar si le has enseñado. No somos nativos digitales y tenemos que dar herramientas a nuestros usuarios para que sean nuestra primera arma de defensa ante un ciberataque". Añade García Dujo que entender que un correo es malicioso y saber que es necesario "es algo que hemos trabajado mucho en la compañía y que nos ha dado muy buenos resultados".

> "A mí no me gusta vender miedo. Creo que es mejor explicar los riesgos"

Más que de tecnologías básicas que debe tener cualquier empresa habla Juan manual García Dujo de salud digital, muchas realmente económicas, con las que se pueden cubrir el 80% de los riesgos de ciberseguridad. En primer lugar, menciona el CISO el "tener inventariados tus activos y saber lo que tienes"; un proceso de actualización de parches de seguridad; la concienciación al usuario; la gestión de los usuarios privilegiados; o una buena configuración de tu parque de sistemas son "buenas prácticas que limitan muchos problemas". Además, en el mundo *cloud* se necesita un doble factor de autenticación, que también es bastante accesible, "y como sabemos que nos van a atacar y vamos a tener un problema, necesitamos contar con un proceso de *backup*, y además probado".

Hablando de herramientas, menciona Juan Manuel García Dujo el *firewall* "para controlar qué pasa por tu red", así como una solución de seguridad *endpoint*, que hoy se llama EDR, "que esté bien configurada".

ENTREVISTAS

Mirando hacia adelante

"Simplificar la gestión de nuestra tecnología" es, en opinión del responsable de Cerealto Siro Foods, una de las cosas que echa en falta del mercado. Explica que por más que existan los SIEM y los orquestadores, cada vez se tienen más herramientas, muchas de las cuales hacen cosas parecidas y se solapan, por lo que "creo que necesitamos tecnologías que nos hagan la vida más sencilla".

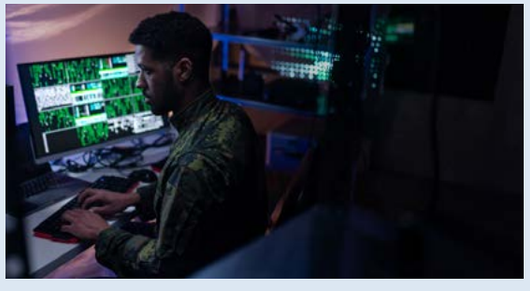
Echando una mirada al futuro, apunta el directivo que las soluciones de gestión de *endpoint*, incluidos los dispositivos móviles "ya están en el mercado, pero creo que son plataformas que han de evolucionar y acabar desplegándose más".

En relación con el mundo de la protección de la información, menciona García Dujo la necesidad de herramientas más transparentes para el cifrado y seguimientos de información, "porque un problema de las tecnologías de seguridad es que sólo se implantan bien cuando son transparentes para el usuario final. Si no, termina teniendo muchos frenos".

Sobre la inteligencia artificial asegura el directivo que no es magia, sino capacidad de cómputo; "al final la inteligencia artificial se basa en que tú hayas entrenado un sistema mucho y eso te cubre el 90 %, el 80 % o al 70% de tus casos, lo cual te genera muchas ventajas. Pero de cara al futuro veo más importante tener herramientas que nos simplifiquen la vida".

ENLACES DESTACADOS

El 35 % de las vulnerabilidades en los sistemas de control industrial no tiene parches



Ucrania quiere que los ciberataques se consideren crímenes de guerra

Hablan los CISO: los desafíos de ciberseguridad empeorarán en 2023

“Elastic se ha introducido en el mundo de la seguridad con una aproximación XDR”

Elastic es una plataforma de analítica de datos. Parecería poca cosa si detrás de una frase con apenas ocho palabras no estuviéramos hablando de una empresa que con casi once años de vida ha realizado once adquisiciones y está cerca de convertirse en una One Billion Company. El camino no ha sido fácil, pero un trabajo bien hecho en la integración de las compras realizadas, una apuesta firme por mercados como el *cloud* y la seguridad, y fichar profesionales como María Campos para el sur de EMEA allanan el camino.

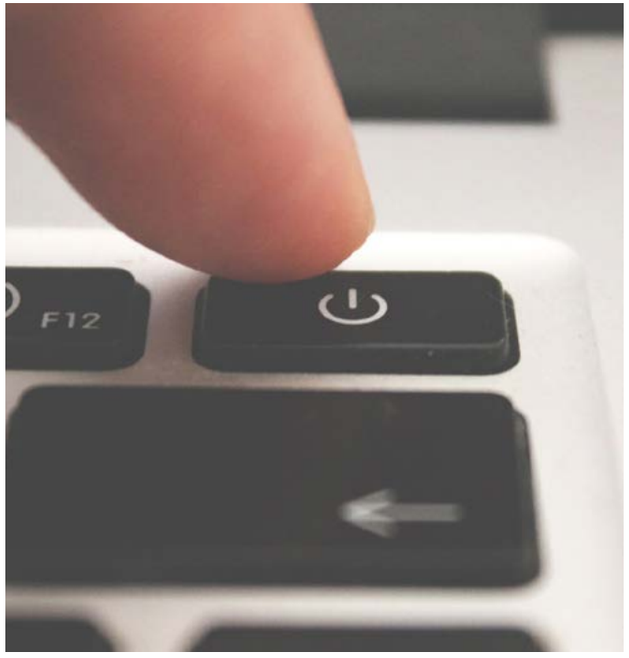
María Campos, Regional VP South EMEA, **Elastic**

Elastic nació en febrero de 2012. Hasta mayo de 2018 recaudó 163 millones de dólares en cinco rondas de financiación y desde octubre de 2018 cotiza en la Bolsa de Nueva York. La compañía tiene casi 20.000 clientes, y teniendo en cuenta que cada vez más empresas están trasladando sus datos a la nube y adoptando nuevas soluciones en la nube, la demanda de búsqueda aumentará, lo que augura un buen futuro a la compañía.

Elastic comenzó como una empresa de búsqueda y ha ampliado su alcance a la observabilidad y la seguridad, dos segmentos bastante candentes en el mercado de TI actual.

Tras casi un año como vicepresidenta de Elastic para el Sur de EMEA, dice María Campos que cuando decidió embarcarse en “la aventura Elastic” evaluó dos cosas, por un lado, el *offering*/ visión estratégica de la compañía y, por otro, el

momento en que se encontraba Elastic como compañía; "viendo lo que ha pasado en estos meses, la buena noticia es que 'esto va por el buen camino'", asegura.



Un camino que cuenta con el reconocimiento que ha recogido la compañía por parte de consultoras y analistas tan solo en el último año, cuando Gartner situó a Elastic como líder en el cuadrante Insight Engines, "que es un área de búsqueda en el que nosotros competimos". Pero le hace especial ilusión a María Campos el reconocimiento de Forrester, "que también en diciembre nos ha situado como líderes en Security Analytics Platform, para toda la parte de SIEM", que es un terreno en el que Elastic se embarcó hace solo dos o tres años. Además, Forrester también ha reconocido la labor de la compañía en el área de AI for IT Operations (AIOps), "que es un área de observabilidad donde Elastic tiene una propuesta muy interesante".

Los reconocimientos se acompañan con cifras. La compañía cerrará su año fiscal en 2023, cuando se prevé que alcance una facturación de 1.000 millones de dólares. Los resultados del segundo trimestre mostraron un crecimiento del 28 %, con especial interés en la parte *cloud*, que creció un 50 % y ya representa el 40 % de los ingresos de Elastic. Destaca, además, un aumento del número de suscripciones de clientes, que ya están cerca de las 20.000. Es decir, desde la perspectiva económica, "Elastic se encuentra en un momento de expansión".

En la región Sur, de la que es responsable María Campos, "hemos consolidado el equipo". Comenta la directiva que en España "Somos del orden de cien personas. No solo tenemos la oficina comercial, sino que hay gente de producto, de desarrollo, ingeniería, soporte, servicios", lo que demuestra que, para Elastic, "Iberia es una región muy potente".

> Elastic comenzó como una empresa de búsqueda y ha ampliado su alcance a la observabilidad y la seguridad, dos segmentos bastante candentes en el mercado de TI actual

Plataforma de analítica

Simplificándolo mucho, Elastic es una plataforma de analítica de datos. La búsqueda, la Observa-

bilidad y la Seguridad son los tres grandes negocios de la plataforma, que es más conocida por las búsquedas.

La Observabilidad consiste en garantizar y tener una visibilidad de todos los sistemas IT, todas las aplicaciones, toda la infraestructura, y prever anomalías. Elastic Observability "tiene una huella bastante potente en el mercado español", explica María Campos, añadiendo que el uso de la plataforma para el mercado de Seguridad es la gran apuesta de la compañía. La presencia de Elastic en este mercado es reciente, "apenas unos tres años desarrollando e integrando soluciones". Explica María Campos que el gran potencial de Elastic es su capacidad para analizar volúmenes de datos elevadísimos dando respuestas en tiempo real o casi real y resultados muy relevantes, "y cuando pensamos que al final la seguridad es analizar datos de seguridad y que, por ejemplo, para algo como el Threat Hunting, analizar volúmenes de datos masivos obteniendo resultados relevantes en un tiempo muy pequeño es vital, te das cuenta de que facilitas mucho la vida de ciertos analistas".

Elastic Security

Elastic cree que la búsqueda es la forma más natural para que las personas interactúen con los datos y está promoviendo un único panel de control de sus datos, con fácil ingesta y aprendizaje automático, lo que permite la colaboración entre los equipos de desarrollo, operaciones y seguridad. Esto coloca a Elastic en la convergencia de dos de los mercados SaaS más populares, la observabilidad y la seguridad, y están invirtiendo fuertemente para capitalizar esta tendencia.

"Elastic se ha introducido en el mundo de la seguridad con una aproximación XDR, donde hay básicamente tres patas: el SIEM, el *endpoint* y el *cloud*", asegura María Campos. EL SIEM es el core de la plataforma de analítica de datos que se ha transformado en correlacionar reglas de seguridad, en añadir toda la capacidad de prevención, detección, respuesta. El potencial del *endpoint* procede de la compra de Endgame en 2019, y la parte de *cloud* se basa en la compra, el año pasado, de tres compañías. Esto lleva a María Campos a asegurar que "nuestra aproximación XDR

ciberseguridadTIC

TAI editorial

ENTREVISTAS

> "La mejor forma de consumir Elastic es en *cloud*, pero nosotros no somos el *driver*"

al final se basa en integrar la telemetría de múltiples dispositivos, todo tipo de fuentes, todo tipo de datos, una forma bastante simple, analizarlos, correlacionarlos y emitir resultados. Ser capaces de tomar decisiones". La base, por tanto, es un SIEM enriquecido con toda la parte de *endpoint* y la de *cloud* security que permite sacar resultados mucho más completos.

Si bien esto le presenta a Elastic una gran oportunidad, también ha aumentado la competencia, tanto dentro como entre categorías. Si Elastic es fuerte en el mercado de observabilidad y se está adentrando en el mercado de seguridad, Splunk, uno de sus competidores, está haciendo el camino contrario; es fuerte en seguridad y está queriendo posicionarse en el de observabilidad.

Al mismo tiempo, no hay que esperar que el mundo del EDR se quede de manos cruzadas esperando que las plataformas de analítica de datos le quiten el negocio. CrowdStrike pasa de la seguridad a la observabilidad al mismo tiempo que Elastic pasa de la observabilidad a la seguridad. El mundo de la protección *endpoint*, desde CrowdStrike pasando por SentinelOne, Sophos, Bitdefender y tantos otros, reconocieron hace un tiempo que la seguridad es, en gran medida, un problema de datos y han desarrollado capacidades que les permiten ingerir y analizar grandes cantidades de datos. No es otra cosa que el mundo de EDR/XDR. CrowdStrike adquirió Humio para este propósito y SentinelOne adquirió Scalyr, y ambas soluciones encontrarán uso en observa-

ENTREVISTAS

Hace tiempo que se sabe que la seguridad es, en gran medida, un problema de datos y se han desarrollado capacidades que permiten ingerir y analizar grandes cantidades de datos

bilidad y SIEM. CrowdStrike sugirió que los CIO y CISO prefieren plataformas que les permitan consolidar agentes, reducir la complejidad, simplificar las operaciones y reducir los costos. Esto incluye reemplazar la gestión de registros heredada y los productos SIEM, y eso representa una amenaza importante para negocios como el de Elastic, que respondió al problema con la compra de Endgame en 2019 y apostando por el *cloud*.

El modelo de consumo de Elastic, por su parte, donde no impacta el número de agentes que se utilicen para recabar los datos necesarios para dar una respuesta ante una amenaza, puede impactar en los proveedores de soluciones EDR.

Ventajas competitivas

Elastic tiene tres ventajas competitivas. Por un lado, es una plataforma unificada, lo que significa

que las soluciones de búsqueda, de observabilidad y de seguridad están disponibles en una plataforma horizontal donde hay un *data lake* de datos “que no tengo que duplicar cuando voy a hacer análisis para la observabilidad o cuando voy a analizarlos desde la perspectiva de seguridad”. Esto es una gran ventaja que impacta en una mejor eficiencia, menor coste y mayor rapidez en la toma de decisiones, “porque no tengo que ir replicando el dato de un sitio para otro”.

La manera de consumir la plataforma es otra de las ventajas de Elastic. Explica María Campos que la plataforma ha ido evolucionando para que se consuma en todo tipo de entornos, desde el *on-premise*, *kubernetes*, en SaaS, en cualquier tipo de *cloud* (AWS, Google y Azure); “cuando nosotros hacemos búsquedas las hacemos con el entorno *on-premise* o entornos *cloud*, y no tenemos que replicar tampoco esos *data lakes*. Ahí somos muy superiores a la competencia, porque con un único *data lake* vamos desplegando nuestros *clusters* en nuestras nubes o en nuestros entornos, pero hacemos un único *data lake* sin necesidad de replicar datos continuamente.

ENTREVISTAS

Y esto se traduce no solo en sencillez, sino en reducción de costes".

El tercer punto que destacar es la manera en que se licencia Elastic. No se licencia por volumen de datos, sino por los recursos que se van a necesitar utilizar en el *cluster*, de forma que, "si optimizamos bien los *clusters*, llegamos a modelos mucho más eficientes comparados con nuestra competencia".

Es decir, podrás poner todos los agentes que quieras, donde quieras, que enviarán la telemetría al *cluster*. Esto hace que Elastic pueda utilizase no sólo como solución principal, sino como solución complementaria de otras soluciones, como puede ser un EDR. Al pagar por el número de nodos del *cluster* de Elastic, dará igual que el agente esté en 10.000, 20.000 o 50.000 *endpoints*, incluidos el IoT, "lo que es una forma de ser mucho más eficiente en costes".

Cliente

¿Quién es el cliente tipo de Elastic? Venir del mundo *open source* y poder servir para múltiples casos de uso hace que haya un Elastic por cada cliente. Dice María Campos que el *open source* está bien para empezar, pero que cuando quieres profesionalizar, lo habitual es adquirir una suscripción que te ofrecerá un nivel de soporte, de servicio y de respuesta.

"El foco comercial de Elastic son las empresas grandes, hasta el *midmarket*. Estamos en las Fortune 500, y en lo que llamamos el mercado Enterprise, con nuestras tres soluciones", además de en todo tipo de industrias. Al respecto, en la página de Elastic se pueden ver casos de éxito en Airbus, Docker o Auchan en la parte de Búsquedas; a Zurich, Fitbit o Telefónica en la parte de Observabilidad; y a Orange, Barclays o NetApp en la parte de Seguridad.

Tiene claro la directiva que "la mejor forma de consumir Elastic es en *cloud*, pero nosotros no

> "Si vas analizando cada adquisición que hemos realizado ves que se han convertido en piezas de lo que es la plataforma Elastic"

somos el *driver*". Explica que, si un cliente ya ha decidido que su estrategia es *cloud*, es muy sencillo subir las cargas de Elastic Cloud y disfrutar de Elastic as a Service "porque es mucho más sencillo, no tiene tiempos de caída, se despreocupa de todo y si haces el TCO a tres años te salen los números".

La acogida del mercado por la apuesta *cloud* de Elastic la demuestran los números: un 40 % de los ingresos de la compañía provienen del *cloud*. El *time-to-market* y flexibilidad que ofrece el *cloud* no te lo da ninguna otra cosa, "pero hay que acompañar bien al cliente en ese viaje inicial".

Adquisiciones

En diez años de vida Elastic ha realizado once adquisiciones. ¿Cuál cree que ha sido más importante?

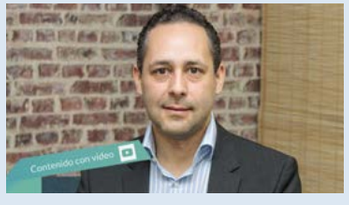
Hay dos líneas que impulsan a Elastic, y por donde María Campos ve el futuro de la compañía. Una es el *cloud*, es decir, Elastic-as-a-Service, y por otro lado la seguridad. Recuerda la directiva que en 2015 Elastic compró Found, que fue la precursora de lo que hoy es Elastic Cloud "y que dirigió muy bien el camino hacia donde estamos hoy".

En la parte de seguridad se compró Perched, que sentó la semilla de la ciberseguridad en una empresa muy centrada en la observabilidad. El mismo año, 2019, se compró Endgame, "y tener SIEM, los servicios, el *endpoint*, empezó a definir una arquitectura muy potente".

Lo que destaca Campos es la buena labor realizada por la compañía a la hora de integrar las adquisiciones que ha realizado. "Si vas analizando cada adquisición ves que se han convertido en piezas de lo que es la plataforma Elastic", dice Campos.

ENLACES DESTACADOS

Secure&IT: "La respuesta ante incidentes debe ser técnica, organizativa y jurídica"



"El paso de la criptografía tradicional hacia la protección con algoritmos post cuánticos requiere tiempo" (Utimaco)

VU: "¿Quién nos convenció de que abriendo la app ya estás seguro?"

Hablamos con Sebastian Stranieri, CEO y fundador de VU Security. Hablamos de hoy, y de un mañana que busca simplificar al máximo la identificación y autenticación del usuario, un futuro en el que la seguridad será dinámica; nuestra identidad la suma de atributos a los que permitiremos acceder, o no; y en el que las grandes corporaciones podrán convertirse en proveedores de identidad.

Sebastian Stranieri, CEO & Founder, **VU Security**

Sebastian Stranieri es el CEO y fundador de VU Security, una compañía especializada en prevención de fraude y protección de identidad fundada en 2006, y que hasta julio de 2021 ha acumulado 19,5 millones de dólares en nueve rondas de financiación, según datos de Crunchbase.

Hoy, la compañía colabora con las empresas para que puedan establecer una estrategia de ciberseguridad que acompañe a todo el ciclo de digitalización del usuario, con soluciones de *onboarding* digital, soluciones de autenticación con múltiple factor y prevención de fraude. El valor de VU, dice su fundador, es "una oferta unificada y completa que, en caso de brecha de seguridad, te limita las conversaciones a una sola compañía, y no a múltiples".

Con Telefónica Tech se ha lanzado el servicio Access & Authentication, que ya tiene clientes tanto en España como en otros países de Latinoamérica y del que se tienen buenas previsiones de crecimiento para este año. Globant es otro de los grandes aliados de la compañía, a los que VU apoya en la búsqueda de oportunidades tanto en España como en Italia.

El valor de VU es una oferta unificada y completa

Este año VU Security busca fortalecer su presencia en los países en los que ya está presente y abrir nuevos mercados "siguiendo los planes estratégicos de nuestros canales. Por ejemplo, con Telefónica en Reino Unido y con Globant a medida que vaya abriendo las operaciones, como hizo en Italia o Alemania". A nivel mayorista se trabaja con Lidera, que ayudará a la compañía a ampliar mercado en España y Portugal.

Mirando hacia el futuro

Mientras la compañía se extiende y hace negocios, mira hacia el futuro. Y de eso hablamos con el fundador de VU Security. La situación actual, explica Sebastián Stranieri es un individuo con un dispositivo que cada vez que tiene que identificarse para el acceso en un servicio, tiene que escribir su nombre de usuario y contraseña. Pero esto no durará para siempre.

El nuevo modelo propuesto por el directivo plantea un usuario con distintos atributos: el atributo licencia de conducir, el atributo cumpleaños, el atributo DNI, el atributo pasaporte... y será el usuario quien otorgue el permiso, o no, de acceder a cada atributo. Si se le requiere el permiso de circulación, mostrará un documento que garantice que su carnet está en regla, y eso no significa que tenga que dar permiso de acceso a la información relativa a su domicilio, o su edad, o su número de teléfono. Además, se tendrá trazabilidad de cada información, de cada dato que se entrega, de forma que en todo momento se sabrá qué organismo

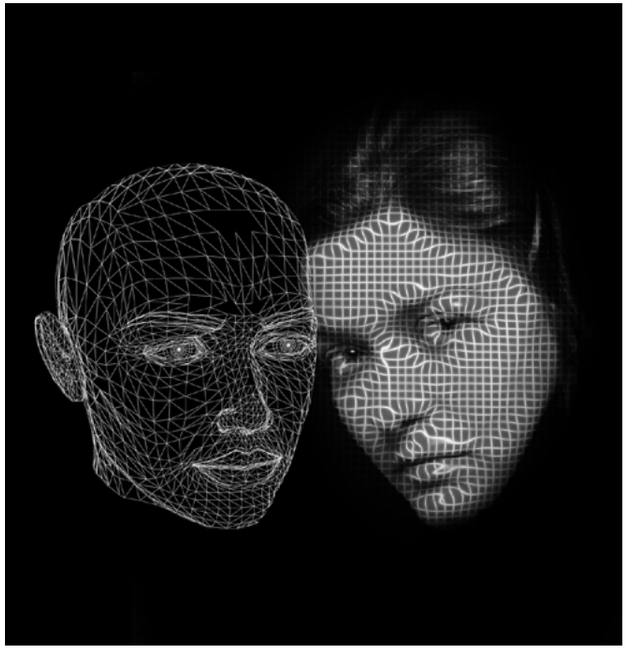
o empresa ha accedido a qué atributo. La información, el dato, podría llevar una marca de agua, de forma que cuando mis datos se vean expuestos, se sepa quién es el responsable de no haberlos almacenado de forma segura.

Explica Stranieri que la identidad de cada uno de nosotros está fragmentada. Y para demostrarlo el CEO y fundador de VU Security plantea un reto: ser capaces de borrar tus datos online en cinco minutos. Algo que asegura que es imposible porque lo que generamos hasta ahora en términos tecnológicos es un caos que solo empeorará, porque el uso de móvil se hace a edades cada vez más tempranas “y toda esa información acumulada va a hacer que cualquiera pueda crear un producto en base a lo que cualquier usuario publica online”, dice el directivo.

“No todo está perdido”, dice también, haciendo referencia al borrador de GDPR 2 y otras regulaciones que están poniendo foco en la descentralización de la identidad. Respecto a esto último explica que lo que se promueve es “centralizar la identidad en el individuo y descentralizarla de las organizaciones”. Explica que por cada servicio que utilizamos somos un perfil y que cada perfil es un fragmento de nuestra identidad. Esa fragmentación impide “ofrecer una buena experiencia de cliente”.

Planteando que tener una identidad desfragmentada mejora la seguridad de la identidad

> A futuro lo que se busca es promover la centralización de la identidad en el individuo y descentralizarla de las organizaciones



En estos modelos de identidades centralizadas que propone Sebastián Stranieri, las compañías querrán convertirse en proveedores de identidad

del usuario porque no te la pueden robar entera, recuerda Sebastián Stranieri que el 98% de los robos de identidad están basados en reutilización de contraseñas. Nunca se sabe cómo va a llegar un ataque, explica el fundador de VU Security. No se sabe si el punto de entrada es un SMS, un *email* o el Whatsapp; "hoy te roban el Whatsapp e inician una campaña de fraude con todos tus contactos", asegura, y eso es porque ninguna de esos elementos está asociado realmente al usuario. "Las cosas que no van a cambiar nunca son tu voz, tu rostro, tu huella, el iris y el ADN, y lo que yo planteo es una mirada de futuro", asegura mientras habla de un futuro no demasiado lejano en el que los teléfonos van a poder procesar video *streaming live* 24/7 de forma que cuando el usuario vaya a estar realizando una operación "podrá validarse constantemente que es quien dice ser, y no solo cuando abra una aplicación" porque, como plantea Sebastian Stranieri, ¿quién nos convenció de que abriendo una *app* ya estás seguro?

Validación continua

Continuamos hablando con el máximo responsable de VU, quien explica que hay dos formas de afrontar el desarrollo de un producto: seguridad estática y seguridad dinámica. Una contraseña, un simple chequeo al inicio de una aplicación, es seguridad estática. Lo que propone el directivo es una seguridad dinámica que llegue a medir las micro-expresiones del ser humano, una seguridad que pueda levantar un *pop-up* en la pantalla y medir qué están viendo tus ojos, por ejemplo, de forma que "puedo estar validando constantemente que la persona es quien dice ser".

En estos modelos de identidades centralizadas que propone Sebastián Stranieri, las compañías querrán convertirse en proveedores de identidad. ¿Qué significa esto? Que si un banco tiene 500 millones de clientes, podría convertirse en el validador de la identidad de esos usuarios

en cualquier espacio, de forma similar a como ahora mismo se pueden utilizar las credenciales de una red social o cuenta de correo electrónico para acceder a otros servicios. Y quien habla de un banco, habla de una gran entidad, incluso de un ayuntamiento o comunidad, que podría proporcionar a todas las tiendas de la región este sistema de autenticación.

¿Cuántas empresas en España son lo suficientemente maduras para adoptar este sistema? Son varias, responde el fundador de VU, quien habla también de "una carrera para ver quién llega primero al consumidor". La compañía ya trabaja en dos pruebas de concepto al tiempo que asegura que "es fundamental que la parte de identidad descentralizada esté dentro de la evaluación de cualquier equipo de investigación y desarrollo por dos aspectos: privacidad e innovación. Imagínate poder registrarte en ese proveedor de identidades y no tener que volver a registrarte nunca más".

Recuerda el directivo que todos los sensores que tienen los dispositivos, y que todo quedaría almacenado y registrado en una red *blockchain*. Lo cierto es que la gestión de identidad, desde el *onboarding* digital hasta la su gestión y los accesos, tanto de usuarios como de perfiles privilegiados, se está convirtiendo en uno de los segmentos de mercado más dinámicos. No solo por los procesos de consolidación, sino porque saber quién accede a qué y desde dónde debe ser parte fundamental de cualquier estrategia de ciberseguridad. CST

ENLACES DESTACADOS

Ransomware, robo de identidades y ataques a API, lo que nos espera en 2023

A cuatro de cada diez usuarios le preocupa por el robo de su identidad

Identidad digital, la importancia de saber protegerla

La protección de la identidad pasa por el certificado digital como opción segura y precisa

Check Point: “Los clientes demandan cada vez más que las soluciones de seguridad sean seguras y efectivas”

A punto de cumplir 30 años de existencia, Check Point Software sigue al pie del cañón. A Gil Schwed, fundador de la compañía, se le atribuye la invención del primer *firewall* y desde entonces la empresa ha continuado innovando. La creciente conectividad de nuestro mundo ha generado en un número creciente de ciberataques que impulsan un mercado mil millonario y plagado de retos.

Mario García, director general de **Check Point Software**

“Hacemos los productos más seguros”, dice Mario García, director general de Check Point para la región de Iberia, cuando le preguntamos por el secreto para mantenerse casi 30 años en el mercado dando beneficios y cumpliendo las expectativas de *partners* y clientes. Comenta, además, que Check Point es la empresa que quieres tener cuando te atacan “porque el producto es realmente bueno y está pensado para que sea seguro, y además fácil de utilizar”.

Explica el directico que la compañía tiene dos tipos de clientes, los que compran un par de productos al año, “y los que tienen un montón de cosas con nosotros, que son quienes aprecian la profundidad del producto y saben que llevamos 30 años mejorando, 30 años añadiendo requisitos de nuestros clientes para que se adecúen a lo que ellos van haciendo”.

ciberseguridadTIC

Tai editorial

ENTREVISTAS

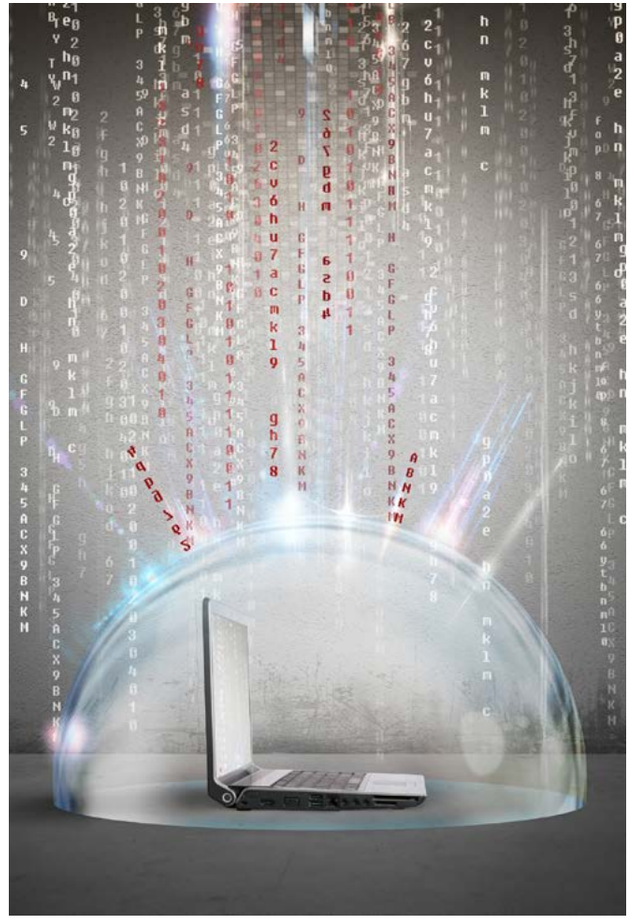
Check Point tiene tres líneas principales de productos que cubren Seguridad de red (Quantum), Seguridad en la nube (Cloudguard) y Seguridad de acceso de usuarios (Harmony). Quantum incluye una serie de *Firewalls*, *Web Gateways* y puntos de acceso que monitorizan e inspeccionan continuamente el tráfico de la red para mitigar las amenazas. Su segunda línea de productos, Cloudguard, tiene como objetivo proteger la nube en varios entornos de múltiples nubes, desde AWS hasta Azure. Finalmente, tenemos Harmony, que utiliza una metodología de Zero Trust para garantizar que el acceso de los usuarios sea seguro.

Nos cuenta Mario García que el de Quantum es el negocio que sigue pesando más en las cuentas de la compañía. Añade que la aparte de *cloud* crece mucho, y que crece "según somos capaces de ir explicando a los clientes que un proyecto de seguridad serio en la *cloud* requiere una serie de necesidades, y que esas necesidades tienen que estar bien cubiertas por un software profesional dedicado, con capacidad y con experiencia. Cuando explicas eso, lo van comprando".

> "No sé por qué, pero la gente piensa que en el móvil no le van a atacar y no hace nada al respecto"

En cuanto a Harmony, está creciendo bastante rápido, y además "con referencias buenísimas en la parte móvil", que sigue siendo la asignatura pendiente en los programas de seguridad de la mayoría de las empresas. "No sé por qué, pero la gente piensa que en el móvil no le van a atacar y no hace nada, o pone un sistema de gestión (MDM – Mobile Device Management) creyendo que por saber cuántos dispositivos tiene, éstos están seguros".

¿Qué peso tiene Infinity en la propuesta de valor de Check Point? Infinity, explica Mario García, se traduce en dos cosas. Por un lado, una plataforma tecnológica, y por otro, en una forma diferente de comprar. "Como plataforma tecnológica tenemos muchísimos clientes por-



ciberseguridadTIC

tai editorial

> "El cliente no solo quiere que le digas que le están atacando, no solo quiere que le avises, quiere que hagamos algo"

que empiezan a ver que la consolidación quita muchos dolores de cabeza, que los recursos son escasos y que utilizarlos mejor aporta mucho valor", explica el directivo, añadiendo que cuando tienes soluciones que hablan entre ellas todo se vuelve mucho más sencillo "y eres inherentemente más seguro".

En cuanto a la forma diferente de comprar, se refiere Mario García a Infinity Total Protection, un nuevo modelo de consumo que la compañía lanzó en enero de 2018 y que incluye tanto hardware como software de protección de red, con defensas totalmente integradas para *endpoints*, *cloud* y móviles y prevención de amenazas de día cero, junto con una gestión unificada y soporte premium 24/7.

Hace años que Check Point tiene identificada una evolución de los ataques, y hace tiempo que asegura que hay una distancia entre las defensas que tienen las empresas y los ataques que reciben. Dice Mario García que cada vez hay más gente que mejora su nivel de seguridad, y por tanto está más protegida, "pero sigue habiendo una gran masa de clientes que ni de lejos están en esa categoría" y que siguen teniendo una conversación centrada en infraestructura, en si una máquina es más o menos grande, o más o menos más rápida; "son conversaciones que no aportan valor", dice el directivo. "Cuando nos encontramos

con interlocutores que quieren hablar de seguridad nos va fenomenal", dice.

Mercado

"Además de consolidación, lo que los clientes están demandando, cada vez más, es un cambio de aproximación en la seguridad. El cliente no solo quiere que le digas que le están atacando, no solo quiere que le avises, quiere que hagamos algo", asegura Mario García. Es lo que en Check Point llaman Protect y es lo que lleva al directivo a asegurar que los clientes empiezan a demandar que las soluciones de seguridad sean seguras y efectivas.

Se prevé que el mercado de ciberseguridad alcance 160.000 millones de dólares, de los que 86.000 millones estarán dedicados a servicios. ¿Cómo está afrontando Check Point esa demanda? "Nuestra razón de ser es la tecnología, y los servicios se despliegan a través del canal de distribución", responde Mario García. Respecto al canal, busca la compañía "gente que tenga capacidad de desplegar servicios sobre nuestras

Quantum, el negocio de seguridad de red, es el negocio que sigue pesando más en las cuentas de Check Point

plataformas, capaz de integrar nuestras soluciones en algo más que una sola reventa, y que sea capaz de ejecutar un proyecto".

¿Y qué os demandan los *partners* que tienen que desplegar sus servicios sobre vuestras soluciones? "Que las soluciones sean más fáciles, funcionen mejor y que tengas expertos para que les ayuden en determinadas situaciones de tal manera que a los *partners* les resulte más fácil trabajar contigo".

ENTREVISTAS

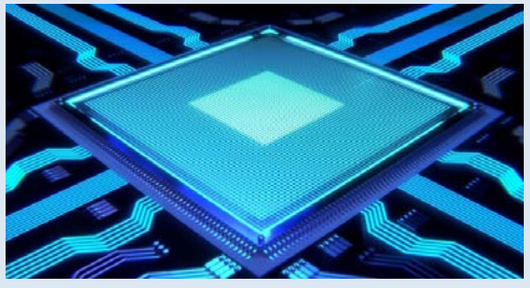
Adquisiciones

En sus 30 años de historia la compañía ha realizado 17 adquisiciones que le han llevado del mundo del *firewall* a la seguridad del *cloud* y el *endpoint*, entre otras. En los últimos años suenan las compras de Dome9, ForceNock, Cymplify, Protego, Odo, Avanan o Spectral. ¿Cuál cree que ha tenido más impacto en la evolución de la compañía? Responde Mario García que Avanan, que es la evolución del CASB (Cloud Access Security Broker), está teniendo un éxito comercial enorme.

Sobre la compra de Dome9 hace unos años, que permitió a Check Point reforzar su propuesta de seguridad en la nube, menciona Mario García que ahora de lo que se habla es de CNAPP (Cloud Native Application Protection Platform), una propuesta por la que apuestan aquellas empresas que empiezan a tener muchos activos en la nube y necesitan "tener soluciones profesionales que sean capaces de decirte qué tienes en la nube y si lo tienes mal, si está bien conectado... y que además sean fáciles de usar".

También comenta las oportunidades que hay en el mundo de *kubernetes* y *shift left*, una metodología que busca introducir la seguridad en el desarrollo cuando antes, y que Check Point ya está comercializando gracias a la compra de Spectral, realizada el año pasado. CST

ENLACES DESTACADOS



Check Point Software e Intel se unen en la lucha contra el *ransomware*

Hablan los CISO: los desafíos de ciberseguridad empeorarán en 2023

Predicciones de ciberseguridad para 2023: más ataques globales, regulación gubernamental y consolidación

“Isoph Cybersecurity destaca por un lenguaje súper sencillo y un precio muy agresivo”

Experta en fraude en tarjetas y medios de pago, Botech lleva años reinventándose. Incluso les ha dado tiempo a cambiar de nombre. El mercado tradicional de la compañía ha sido el financiero, pero hace mucho tiempo que innovan, y aunque hace menos que se fijaron en la pyme, los avances realizados son destacables. También tienen tiempo de invertir en nuevas aventuras, la última se llama Solver4 y es el primer SOC virtual a nivel mundial especializado en PCI DSS 4.0.

Miguel Ángel Rojo, CEO **Botech**

En 2006, las compañías American Express, Discover Financial Services, JCB International, MasterCard y Visa formaron una organización llamada PCI Council (Payment Card Industry Security Standards Council) con el objetivo mejorar la seguridad en las transacciones online y garantizar la trazabilidad del dinero y de los titulares de pago. De ahí surgió la normativa PCI DSS (Payment Card Industry Data Security Standard) que es obligatoria para cualquier empresa que maneje datos de pago a través de tarjetas.

Como empresa experta en fraude en tarjetas y medios de pago, Botech es experta en PCI DSS, hasta el punto de haberse convertido en certificador de la normativa. Nos cuenta Miguel Ángel Rojo, CEO de la compañía, que durante el año pasado se dio un fuerte impulso a la certificación en medios de pago porque “hay un fuerte incremento en la transacciona-

ciberseguridadTIC

Tai editorial

lidad electrónica". Habla Rojo de una "normalización" que ha llevado incluso a las pequeñas empresas a establecer su propia plataforma de ventas y servicios en Internet.

Explica también el CEO de Botech que el aumento del comercio electrónico está generando muchísimo fraude, y está haciendo que las grandes marcas, como son Mastercard y VISA, exijan que el sistema financiero de países como México, donde la compañía tiene presencia, "tiene que ser PCI compliance. Esto exige que los comercios adheridos a los bancos, desde el más grandes al más pequeño, cumplan la normativa siempre que medie una tarjeta bancaria".

Este impulso a la normativa ha llevado a Botech a reforzar el equipo con dos QSA en México, que se suman a los dos que hay en España, además de convertirse en empresa Qualified PIN Assessor (QPA) para la evaluación del cumplimiento de la normativa PCI PIN (Payment Card Industry PIN Security), un estándar que establece los requerimientos para

> El aumento del comercio electrónico está generando muchísimo fraude

la gestión, el procesamiento y la transmisión segura del número de identificación personal (más conocido como número PIN) durante las transacciones de pago. Que sólo haya 167 empresas certificadoras en todo el mundo hace que esta certificación sea bastante exclusiva.

Asegura Miguel Ángel Rojo que la parte de Certificación PIN "te da una visión muy grande, y muy clara, de las necesidades de una compañía, con lo cual nos permite hacer up-selling

ENTREVISTAS

PCI 4.0 añade mayores niveles de exigencia en la parte de certificación y será de obligado cumplimiento en marzo de 2024

dentro de la cuenta y vender otros servicios aparte de la parte de PCI", como son los de ciberseguridad.

Como la mayoría de las normativas, la PCI evoluciona. Todo lo que está abordando Botech este año ya es conforme PCI 4.0, que será de obligado cumplimiento en marzo de 2024 y añade "mayores niveles de exigencia en la parte de certificación". Explica Migue Ángel Blanco que no es que antes la normativa fuera laxa, sino que "se va endureciendo porque el fraude es exponencial, el ciberdelincuente se va inventando cosas nuevas y no te puedes quedar en lo que exigías hace diez años".

Cuidando a la pyme

Botech FPI es la parte de servicios, y Botech Labs es la parte de tecnología y producto, y la apuesta de la compañía para llevar la ciberseguridad al mundo pyme. Una apuesta bautizada como Isoph Negocio Seguro, que incluye Isoph Mobile, Isoph DNS y Isoph Pyme. El objetivo, explica Miguel Ángel Rojo, es "ayudar a las pymes a que tengan unas herramientas súper seguras para protegerse contra ciberataques", y con una idea clara: "que no se utilice lenguaje técnico".

Una vez realizada la consulta, las pymes reciben un nivel de riesgo en forma de termóme-

ENTREVISTAS

tro y una lista de acciones que realizar, y cómo realizarlas, mediante un guía de fácil lectura; se realiza un inventario del software que se ofrece una serie de recomendaciones que van desde actualizar Windows a comprobar que la factura que se va a pagar procede de un proveedor habitual, o saber identificar un correo de phishing.

La última mejora incorporada a Isoph Negocio Seguro busca "filtrar toda la navegación de los usuarios de forma que, si quiere acceder a una página que no debiera, automáticamente bloqueamos la navegación y lanzamos un mensaje, porque hay que proteger la salud de las herramientas de trabajo", explica Miguel Ángel Blanco.

Con Isoph Mobile, se lleva la seguridad a los dispositivos móviles. Algo muy necesario si tenemos en cuenta que muchos comerciales "usan los dispositivos móviles para resolver pedidos", los mismos dispositivos que a veces están en manos de los más pequeños de la casa.

Isoph Payment busca dar soporte al comercio electrónico de las pequeñas empresas

Y si toda la protección en el mundo pyme se ha centrado en Windows, en la parte móvil se ha centrado en Android e iOS, "que es el grueso de la industria, donde nosotros queremos enfocarnos, porque le hemos puesto un precio muy competitivo y accesible para todo el que quiera que sus equipos estén protegidos".

"Un lenguaje súper sencillo y un precio muy agresivo" son los dos elementos que, en opinión de Miguel Ángel Rojo, destaca de Isoph Cybersecurity.

Isoph Payment

Si algo caracteriza a Botech es la innovación. La compañía gestó parte de la familia Isoph durante la pandemia, y sigue haciéndola crecer. En la segunda mitad de 2022 la compañía trabajó en Isoph Payment, una tecnología de prevención de fraude flexible, con un proceso de integración rápido y sencillo, y un coste económico. La idea detrás de la idea es introducir PCI en los comercios pequeños, "dar soporte al comercio electrónico de las pequeñas

ciberseguridadTIC

Tai editorial

La última propuesta gestada en Botech se llama Solver4, una empresa especializada en el cumplimiento de la normativa PCI DSS 4.0

empresas", y proteger para que "no haya fraude en los contracargos, que es lo que mata al ecommerce pequeño. Que la compra sea segura y no puedas recibir rechazos de material". Isoph Payment se ofrece en modo servicio. Se trata de una solución configurable para cada comercio que permite definir el nivel de riesgo y realiza una monitorización continua de todas las transacciones efectuadas, con un portal administrativo donde se recogen todos los datos de fácil accesibilidad e interpretación.

La propuesta responde a una necesidad. Explica Miguel Ángel Rojo que en nuestro país la mayoría de los pagos se realizan a través de Redsys, pero que a los pequeños comercios les resulta complicado pagar las tasas y se van a otro tipo de plataformas. En México, Botech trabaja con un agregador que tiene 12.000 comercios, y es uno de los 34 que hay; "ese es el público al que queremos ir con Isoph Payment", asegura el directivo.

2022 ha sido intenso. A finales de año la compañía recibió el premio "Madrid Network Award de innovación en ciberseguridad", junto con Funditec, en reconocimiento a un proyecto que arrancó año y medio antes: OREL, plataforma predictiva de propagación de Malware, cuyo principal objetivo es investigar y desarrollar una plataforma tecnológicamente avanzada e interactiva para la detección del malware del sistema operativo Android.

Isoph Cybersecurity

ISOPH Cybersecurity es el paraguas bajo el cual Botech ha desplegado una serie de propuestas para el mercado de pequeña y mediana empresa.

Isoph Pyme. Basado en tecnología Isoph, esta propuesta ayuda a mantener los sistemas actualizados y parcheados. El seguimiento continuo y la recepción periódica de informes permite conocer si existe algún indicio de vulnerabilidad en los sistemas protegidos. Toda la información se gestiona a través de una consola sencilla e intuitiva que muestra el estado de seguridad en tiempo real y permite tomar medidas para prevenir incidentes.

Isoph DNS (Domain Name System) Protection. Tecnología en la nube que, utilizando sistemas de inteligencia artificial, fuentes de inteligencia propietarias y algoritmos avanzados de ciencia de datos, monitoriza en tiempo real las comunicaciones de los sistemas bloqueando las principales amenazas y técnicas de piratería. Además, cada vez que se introduce una URL, impide el acceso a determinadas páginas web o direcciones IP que parezcan sospechosas.

Isoph Business. Tecnología en la nube que realiza un seguimiento continuo de los archivos para saber si han sufrido cambios no autorizados e inesperados. Este escáner de integridad de archivos permite a las organizaciones anticipar y prevenir posibles ataques e infracciones de seguridad.

Isoph Mobile. Ofrece la máxima seguridad para dispositivos Android. La herramienta realiza un rápido análisis en profundidad de los dispositivos Android y permite saber si el terminal ha estado expuesto a algún tipo de vulnerabilidad o amenaza. El servicio está disponible en tres versiones: Gratuito, Empresarial y Ejecutivo.

Isoph Payment. Permite proteger a las organizaciones contra el fraude masivo actual. Se trata de una solución configurable para cada comercio que permite definir el nivel de riesgo. Una tecnología que realiza una monitorización continua de todas las transacciones efectuadas con un portal administrativo donde se recogen todos los datos de fácil accesibilidad e interpretación.

El proyecto, que ha generado “resultados muy interesantes”, anima a la compañía a “seguir con esa política de tener siempre algún proyecto de innovación e investigación orientado a la pyme”. Reconoce aquí Miguel Ángel Rojo que la compañía ha estado muy anclada en el sector financiero, “que en España tiene el tamaño que tiene”, y que se apuesta por el mercado pyme; también que en 2023 quiere poner muchísimo foco en el desarrollo de canal en Latinoamérica, y sobre todo en México porque “creemos que con la madurez que

tenemos en los servicios y la tecnología, podemos acometer un mercado con un volumen interesante".

Solver 4

La última propuesta gestada en Botech se llama Solver4, una empresa especializada en el cumplimiento de la normativa PCI DSS 4.0 que cuenta con el primer SOC virtual a nivel mundial especializado es esta normativa.

PCI DSS es el estándar de seguridad de datos de la industria de que el pasado mes de marzo anunciaba la versión 4.0 con tres novedades destacadas: Implementación de la autenticación de múltiples factores (MFA); la sustitución de la terminología de "*Firewall*" por "controles de seguridad de red" para abarcar más tecnologías de seguridad y tener más flexibilidad; y que gran parte de los nuevos requisitos implican análisis de riesgos específicos.

El VSOC 4.0 cuenta con gestión continua de logs, Red Team, Forenses remotos y servicio de MDR (Managed Detection and Response). Se trata de un SOC pionero creado por el equipo de expertos internacionales de Solver4 cuenta con el *partnership* estratégico de BOTECH como canal de distribución de su servicio y empresa certificadora PCI registrada en el PCI Security Standards Council.

ENLACES DESTACADOS

BOTECH ofrece una protección total a las pymes con Isoph Negocio Ciberseguro

"Trabajamos para que nuestra tecnología evolucione a la par que los ciberataques"

Solver4 y el primer SOC Virtual especializado en PCI DSS 4.0

Tenemos **toda la información** que necesitas